MIT Guide to Lock Picking

Ted the Tool

September 1, 1991

Distributio

Co yright 1987, 1991 Theodore T. Tool. All rights reserved.

Permission to re roduce this document on a non- rofit basis is granted rovided that this co yright and distribution notice is included in full. The information in this booklet is rovided for educational ur oses only.

August 1991 revision.

Co te ts

1 It's Easy **4**

2 How a Key Opens a Lock **5**

3 The Flatland Model **7**

4 Basic Picking & The Binding Defect **9**

5 The Pin Column Model **11**

6 Basic Scrubbing **17**

7 Advanced Lock Picking **21**

7.1 Mechanical Skills 21

7.2 Zen and the Art of Lock Picking 21

7.3 Analytic Thinking 22

8 Exercises **23**

8.1 Exercise 1: Bouncing the ick 23

8.2 Exercise 2: Picking ressure 24

8.3 Exercise 3: Picking Torque 24

8.4 Exercise 4: Identifying Set Pins 25

8.5 Exercise 5: Projection 25

9 Recognizing and Exploiting Personality Traits **27**

9.1 Which Way To Turn 27

9.2 How Far to Turn 29

9.3 Gravity 29

9.4 Pins Not Setting 29

9.5 Elastic Deformation 29

9.6 Loose Plug 30
9.7 Pin Diameter 32
9.8 Beveled Holes and Rounded ins 32
9.9 Mushroom Driver Pins 34
9.10 Master Keys 36
9.11 Driver or S acer Enters Keyway 38
9.12 Vibration Picking 39
9.13 Disk Tumblers 40

10 Final Remarks **42**

A Tools **43**
A.1 Pick Sha es 43
A.2 Street cleaner bristles 44
A.3 Bicycle s okes 46
A.4 Brick Stra 47

B Legal Issues **48**

Chapter 1

It's Easy

The big secret of lock icking is that it's easy. Anyone can learn how to ick locks.

The theory of lock icking is the theory of ex loiting mechanical defects. There are a few basic conce ts and definitions but the bulk of the material consists of tricks for o ening locks with articular defects or characteristics. The organization of this manual re ects this structure. The first few cha ters resent the vocabulary and basic information about locks and lock icking. There is no way to learn lock icking without racticing, so one cha ter resents a set of carefully chosen exercises that will hel you learn the skills of lock icking. The document ends with a catalog of the mechanical traits and defects found in locks and the techniques used to recognize and ex loit them. The first a endix describes how to make lock icking tools. The other a endix resents some of the legal issues of lock icking.

The exercises are im ortant. The only way to learn how to recognize and ex loit the defects in a lock is to ractice. This means racticing many times on the same lock as well as racticing on many different locks. Anyone can learn how to o en desk and filing cabinet locks, but the ability to o en most locks in under thirty seconds is a skill that requires ractice.

Before getting into the details of locks and icking, it is worth ointing out that lock icking is just one way to by ass a lock, though it does cause less damage than brute force techniques. In fact, it may be easier to by ass the bolt mechanism than to by ass the lock. It may also be easier to by ass some other art of the door or even avoid the door entirely. Remember: There is always another way, usually a better one.

Chapter 2

ow a Key Ope s a Lock

This cha ter resents the basic workings of in tumbler locks, and the vocabulary used in the rest of this booklet. The terms used to describe locks and lock arts vary from manufacture to manufacture and from city to city, so even if you already understand the basic workings of locks, you should look at figure 2.1 for the vocabulary.

Knowing how a lock works when it is o ened by a key is only art of what you need to know. You also need to know how a lock res onds to icking. Cha ters 3 and 5 resent models which will hel you understand a lock's res onse to icking.

Figure 2.1 introduces the vocabulary of real locks. The key is inserted into the *keyway* of the *plug*. The rotrusions on the side of the keyway are called *wards*. Wards restrict the set of keys that can be inserted into the lug. The lug is a cylinder which can rotate when the ro er key is fully inserted. The non-rotating art of the lock is called the *hull*. The first in touched by the key is called in one. The remaining ins are numbered increasingly toward the rear of the lock.

The ro er key lifts each in air until the ga between the *key pin* and the *driver pin* reaches the *sheer line*. When all the ins are in this osition, the lug can rotate and the lock can be o ened. An incorrect key will leave some of the ins rotruding between the hull and the lug, and these ins will revent the lug from rotating.

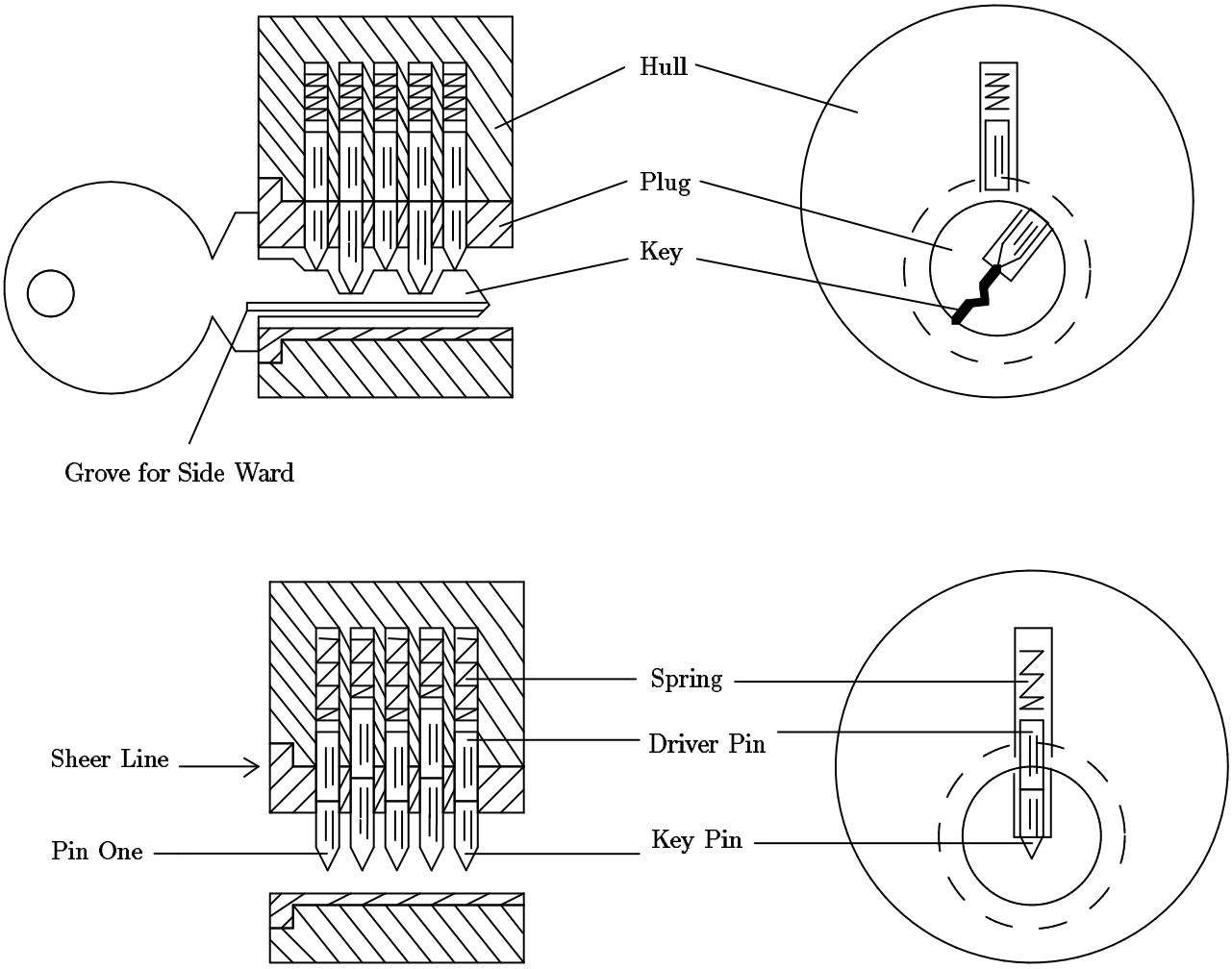


Figure 2.1: Workings of in tumbler locks

Chapter 3

The F at a Mo e

In order to become good at icking locks, you will need a detailed understanding of how locks works and what ha ens as it is icked. This document uses two models to hel you understand the behavior of locks. This cha ter resents a model that highlights interactions between in ositions. Cha ter 4 uses this model to ex lain how icking works. Cha ter 9 will use this model to ex lain com licated mechanical defects.

The " atland" model of a lock is shown in Figure 3.1. This is not a cross section of a real lock. It is a cross section of a very sim le kind of lock. The ur ose of this lock is to kee two lates of metal from sliding over each other unless the ro er key is resent. The lock is constructed by lacing the two lates over each other and drilling holes which ass through both lates. The figure shows a two hole lock. Two ins are laced in each hole such that the ga between the ins does not line u with the ga between the lates. The bottom in is called the *key pin* because it touches the key. The to in is called the *driver pin*. Often the driver and key ins are just called the driver and the in. A rotrusion on the underside of the bottom late kee s the ins from falling out, and a s ring above the to late ushes down on the driver in.

If the key is absent, the lates cannot slide over each other because the driver ins ass through both lates. The correct key lifts the in airs to align the ga between the ins with the ga between the lates. See Figure 3.3. That is, the key lifts the key in until its to reaches the lock's sheer line. In this configuration, the lates can slide ast each other.

Figure 3.3 also illustrates one of the im ortant features of real locks. There is always a sliding allowance. That is, any arts which slide ast each other must be se arated by a ga . The ga between the to and bottom lates allows a range of keys to o en the lock. Notice that the right key in in Figure 3.3 is not raised as high as the left in, yet the lock will still o en.

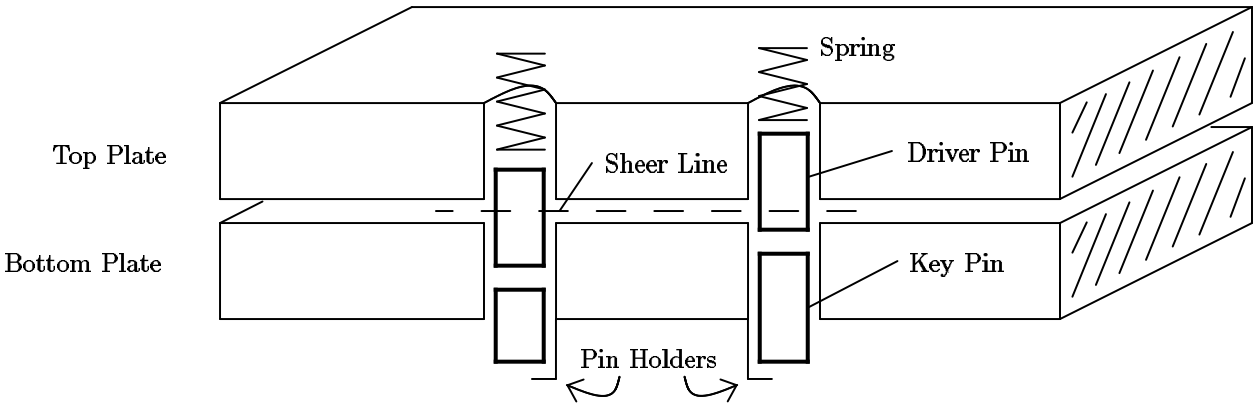


Figure 3.1: Flatland model of a lock

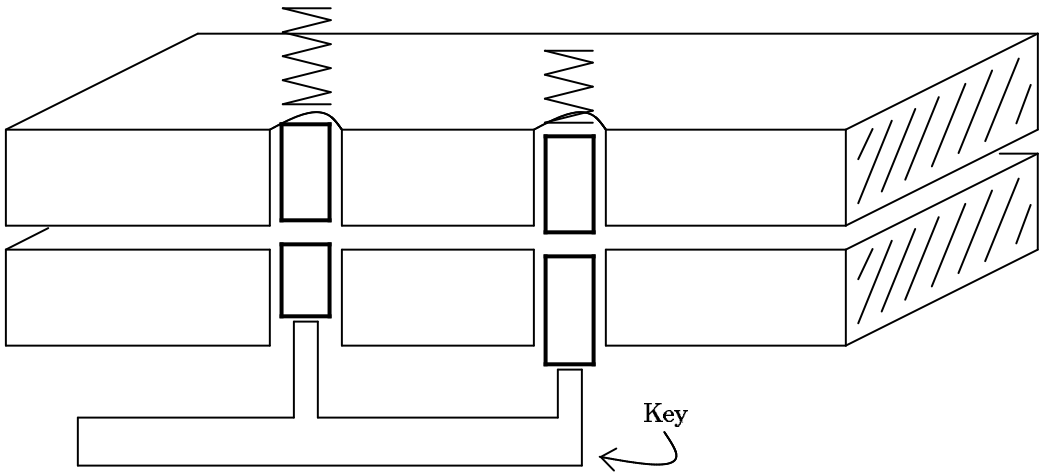


Figure 3.2: (a) Flatland key raises ins

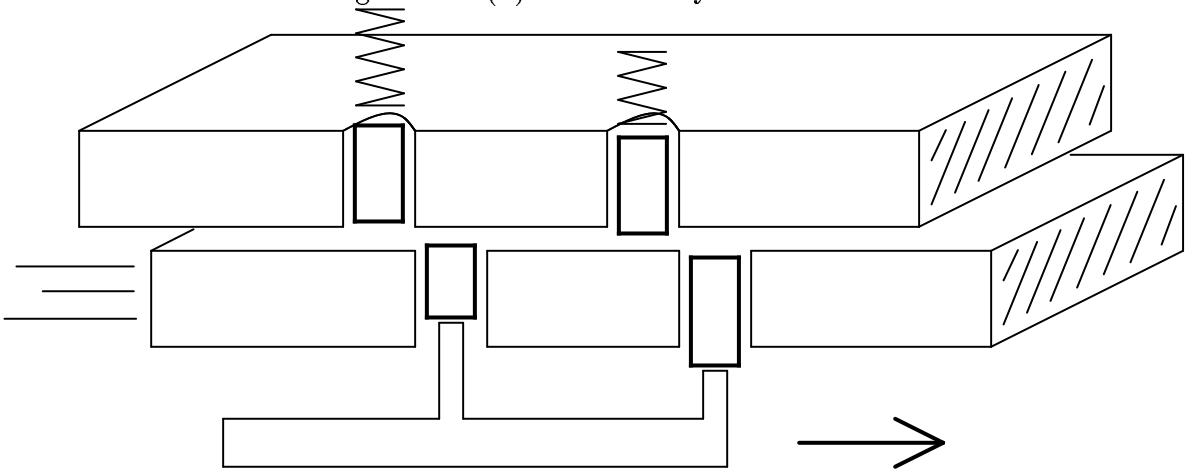


Figure 3.3: (b) Pro er key allows lates to slide

Chapter 4

Basic Picki g & The Bi i g Defect

The atland model highlights the basic defect that enables lock icking to work. This defect makes it ossible to o en a lock by lifting the ins one at a time, and thus you don't need a key to lift all the ins at the same time. Figure 4.3 shows how the ins of a lock can be set one at a time. The first ste of the rocedure is to a ly a sheer force to the lock by ushing on the bottom late. This force causes one or more of the ins to be scissored between the to and bottom late. The most common defect in a lock is that only one in will bind. Figure 4.3a shows the left in binding. Even though a in is binding, it can be ushed u with a icking tool, see Figure 4.3b. When the to of the key in reaches the sheer line, the bottom late will slide slightly. If the ick is removed, the driver in will be held u by the overla ing bottom late, and the key in will dro down to its initial osition, see Figure 4.3c. The slight movement of the bottom late causes a new in to bind. The same rocedure can be used to set the new in.

Thus, the rocedure for *one pin at a time picking* a lock is to a ly a sheer force, find the in which is binding the most, and ush it u . When the to of the key in reaches the sheer line, the moving ortion of the lock will give slightly, and driver in will be tra ed above the sheer line. This is called *setting* a in.

Cha ter 9 discusses the different defects that cause ins to bind one at a time.

1. A ly a sheer force.
2. Find the in that is binding the most.
3. Push that in u until you feel it set at the sheer line.
4. Go to ste 2.

Table 4.1: Figure 5: Picking a lock one in at a time.

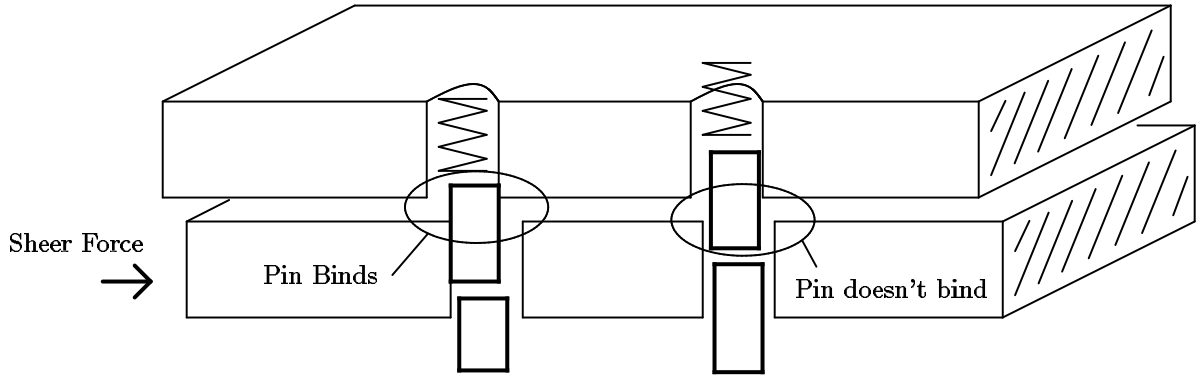


Figure 4.1: (a) Sheer force causes driver to bind

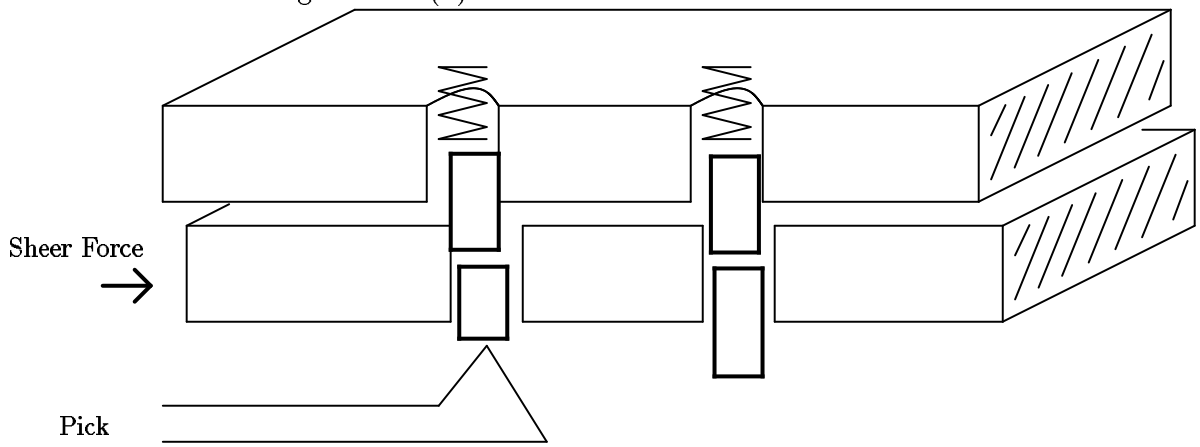


Figure 4.2: (b) Pick lifts the binding in

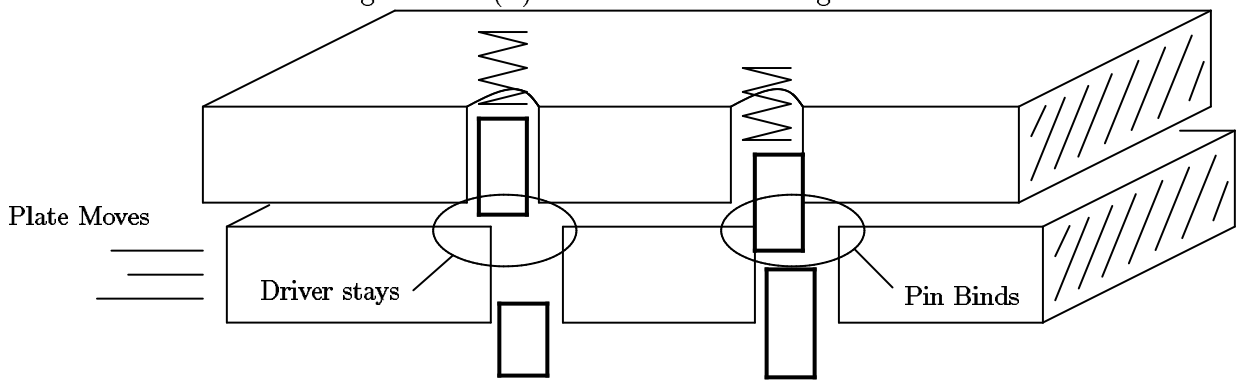


Figure 4.3: (c) Left driver sets and right driver binds

Chapter 5

The Pi Co um Mo e

The atland model of locks can ex lain effects that involve more than one in, but a different model is needed to ex lain the detailed behavior of a single in. See Figure 5.1. The in-column model highlights the relationshi between the torque a lied and the amount of force needed to lift each in. It is essential that you understand this relationshi .

In order to understand the "feel" of lock icking you need to know how the movement of a in is effect by the torque a lied by your torque wrench (tensioner) and the ressure a lied by your ick. A good way to re resent this understanding is a gra h that shows the minimum ressure needed to move a in as a function of how far the in has been dis laced from its initial osition. The remainder of this cha ter will derive that force gra h from the in-column model.

Figure 5.2 shows a single in osition after torque has been a lied to the lug. The forces acting of the driver in are the friction from the sides, the s ring contact force from above, and the contact force from the key in below. The amount of ressure you a ly to the ick determines the contact force from below.

The s ring force increases as the ins are ushed into the hull, but the increase is slight, so we will assume that the s ring force is constant over the range of dis lacements we are interested in. The ins will not move unless you a ly enough ressure to overcome the s ring force. The binding friction is ro ortional to how hard the driver in is being scissored between the lug and the hull, which in this case is ro ortional to the torque. The more torque you a ly to the lug, the harder it will be to move the ins. To make a in move, you need to a ly a ressure that is greater than the sum of the s ring and friction forces.

When the bottom of the driver in reaches the sheer line, the situation suddenly changes. See Figure 5.3. The friction binding force dro s to zero and the lug rotates slightly (until some other in binds). Now the only resistance to motion is the s ring force. After the to of the key in crosses the ga between the lug and the hull, a new contact force arises from the key in striking the hull. This force can be quite large, and it causes a eak in the amount of ressure needed to move a in.

If the ins are ushed further into the hull, the key in acquires a binding fiction like the driver in had in the initial situation. See Figure 5.4. Thus, the amount of ressure needed

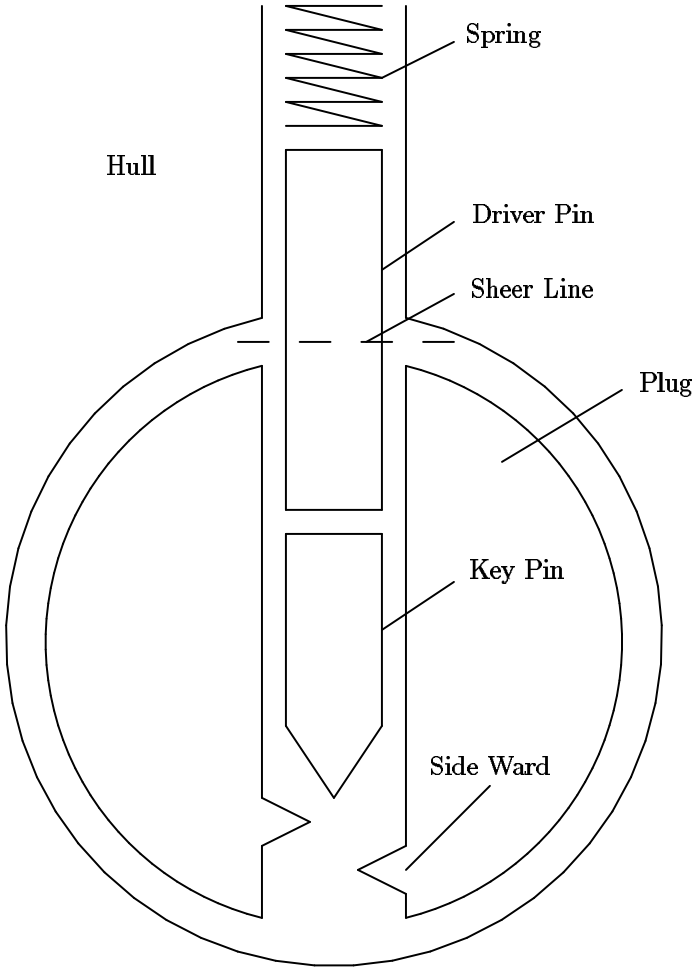


Figure 5.1: The in-column model

to move the ins before and after the sheer line is about the same. Increasing the torque increases the required ressure. At the sheer line, the ressure increases dramatically due to the key in hitting the hull. This analysis is summarized gra hically in figure 5.5.

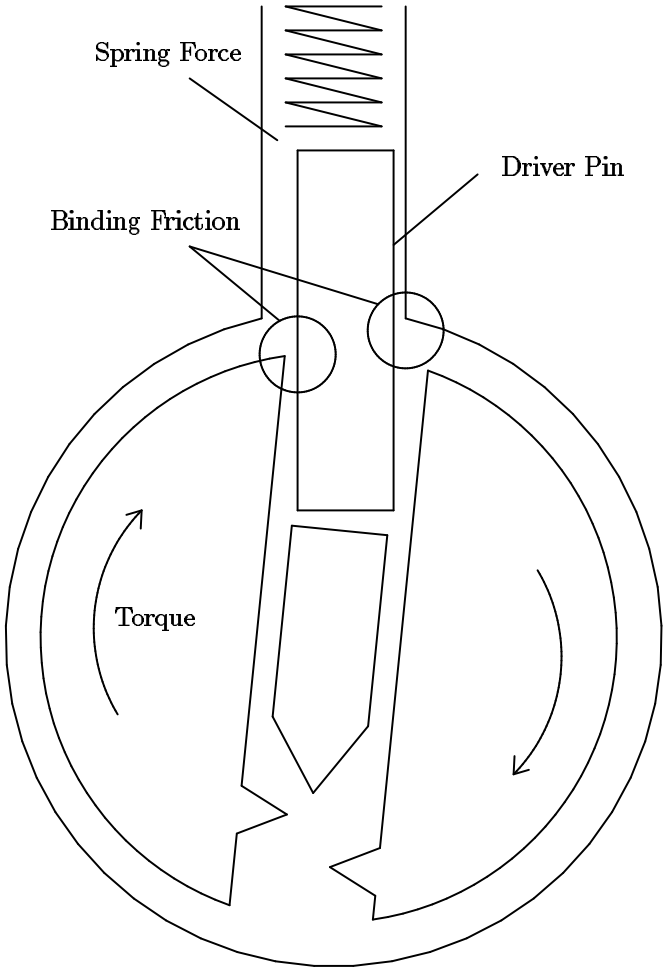


Figure 5.2: Binding in the in-column model

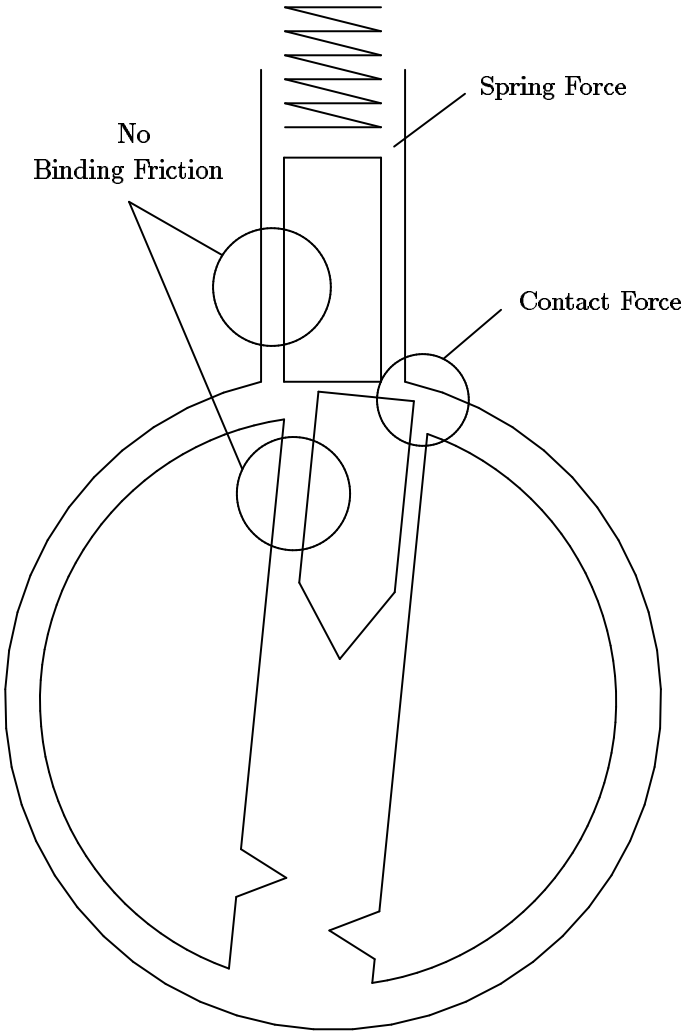


Figure 5.3: Pins at the sheer line

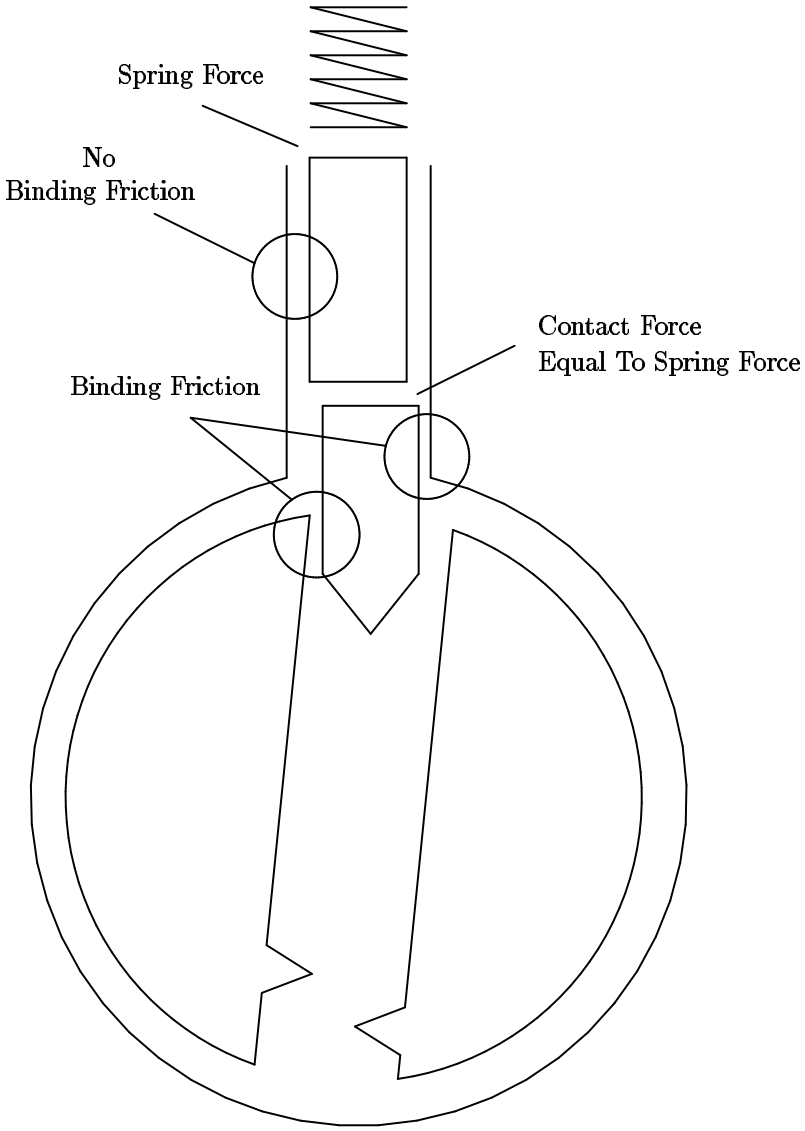


Figure 5.4: Key in enters hull

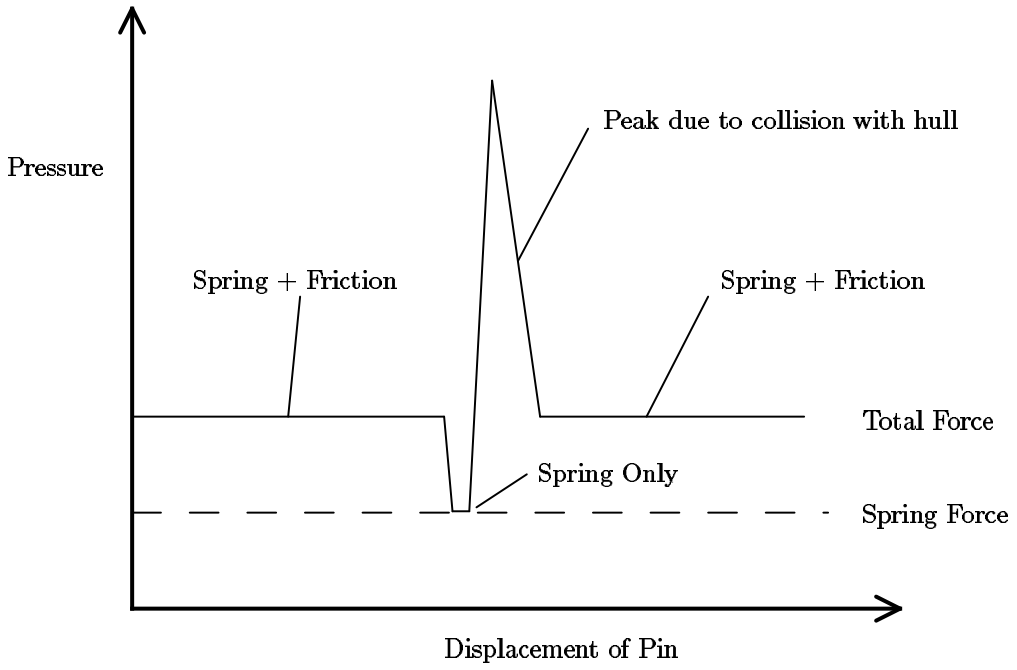


Figure 5.5: Pressure required to move ins

Chapter 6

Basic Scrubbing

At home you can take your time picking a lock, but in the field, speed is always essential. This chapter presents a lock picking technique called *scrubbing* that can quickly open most locks.

The slow step in basic picking (chapter 4) is locating the pin which is binding the most. The force diagram (Figure 5.5) developed in chapter 5 suggests a fast way to select the correct pin to lift. Assume that all the pins could be characterized by the same force diagram. That is, assume that they all bind at once and that they all encounter the same friction. Now consider the effect of running the pick over all the pins with a pressure that is great enough to overcome the spring and friction forces but not great enough to overcome the collision force of the key pin hitting the hull. Any pressure that is above the portion of the force graph and below the top of the peak will work. As the pick passes over a pin, the pin will rise until it hits the hull, but it will not enter the hull. See Figure 5.3. The collision force at the sheer line resists the pressure of the pick, so the pick rides over the pin without pressing it into the hull. If the proper torque is being applied, the plug will rotate slightly. As the pick leaves the pin, the key pin will fall back to its initial position, but the driver pin will catch on the edge of the plug and stay above the sheer line. See figure 6.1. In theory one stroke of the pick over the pins will cause the lock to open.

In practice, at most one or two pins will set during a single stroke of the pick, so several strokes are necessary. Basically, you use the pick to scrub back and forth over the pins while you adjust the amount of torque on the plug. The exercises in chapter 8 will teach you how to choose the correct torque and pressure.

You will find that the pins of a lock tend to set in a particular order. Many factors effect this order (see chapter 9), but the primary cause is a misalignment between the center axis of the plug and the axis on which the holes were drilled. See figure 6.2. If the axis of the pin holes is skewed from the center line of the plug, then the pins will set from back to front if the plug is turned one way, and from front to back if the plug is turned the other way. Many locks have this defect.

Scrubbing is fast because you don't need to pay attention to individual pins. You only need to find the correct torque and pressure. Figure 6.1 summarizes the steps of picking a lock by scrubbing. The exercises will teach you how to recognize when a pin is set and how

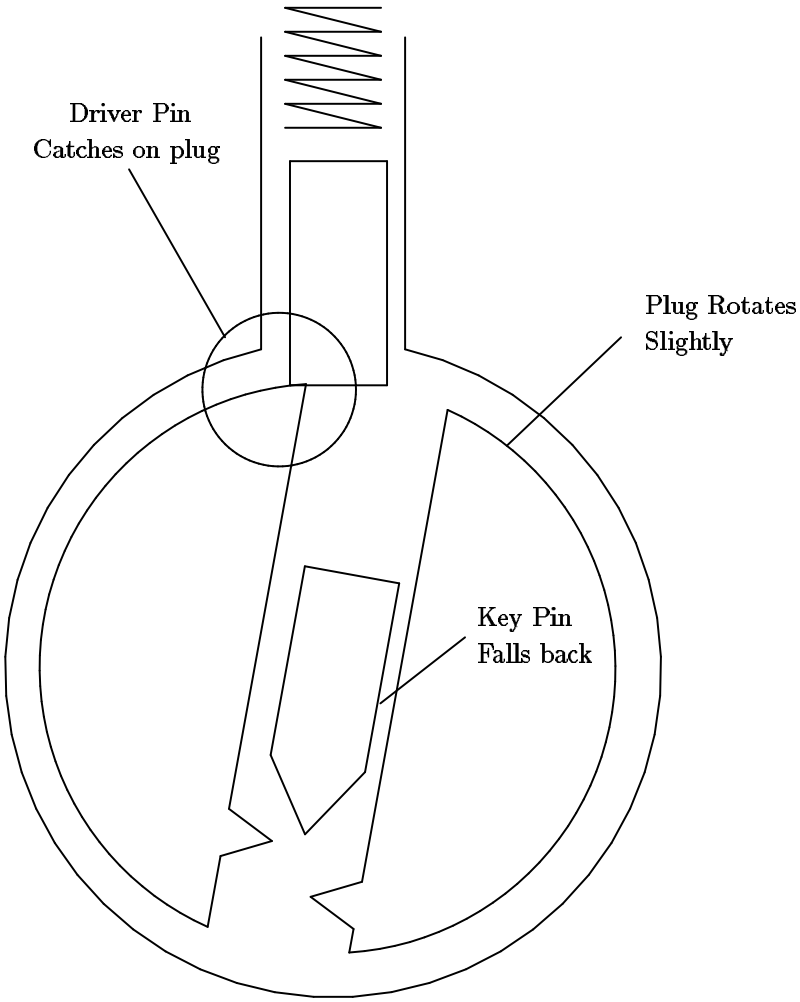
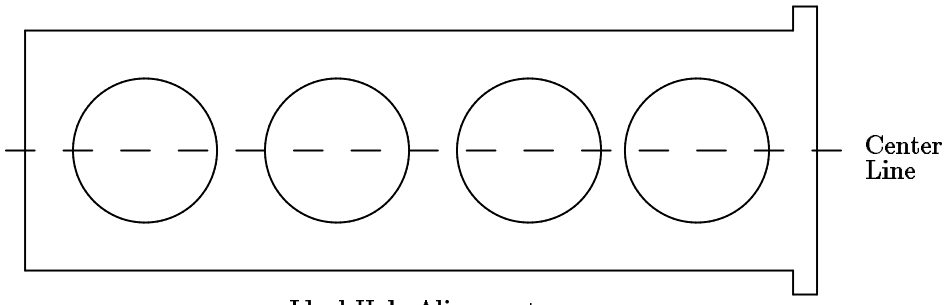


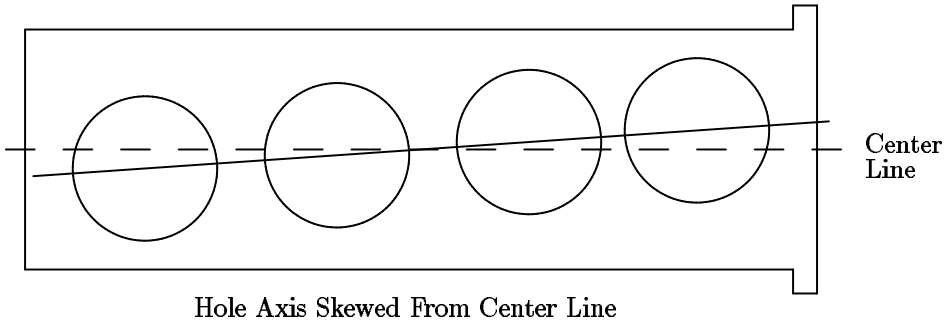
Figure 6.1: Driver in catches on lug

to a ly the correct forces. If a lock doesn't o en quickly, then it robably has one of the characteristics described in cha ter 9 and you will have to concentrate on individual ins.

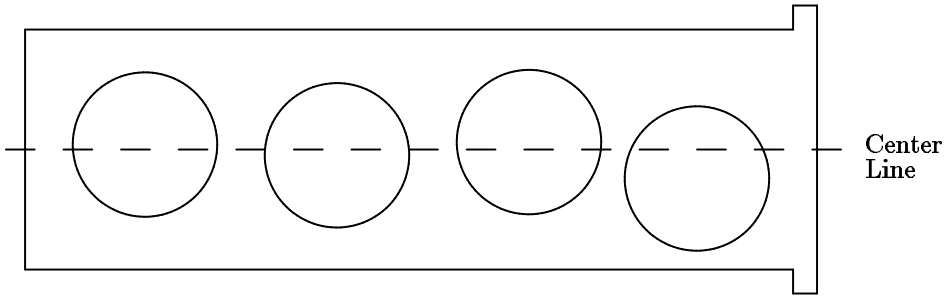
Back Top view of plug Front



Ideal Hole Alignment



Hole Axis Skewed From Center Line



Random

1. Insert the ick and torque wrench. Without a lying any torque ull the ick out to get a feel for the stiffness of the lock's s rings.

2. A ly a light torque. Insert the ick without touching the ins. As you ull the ick out, a ly ressure to the ins. The ressure should be slightly larger than the minimum necessary to overcome the s ring force.

3. Gradually increase the torque with each stroke of the ick until ins begin to set.

4. Kee ing the torque fixed, scrub back and forth over the ins that have not set. If additional ins do not set, release the torque and start over with the torque found in the last ste .

5. Once the majority of the ins have been set, increase the torque and scrub the ins with a slightly larger ressure. This will set any ins which have set low due to beveled edges, etc.

Table 6.1: Figure 13: Basic scrubbing.

Chapter 7

A va ce Lock Picki g

Sim le lock icking is a trade that anyone can learn. However, advanced lock icking is a craft that requires mechanical sensitivity, hysical dexterity, visual concentration and analytic thinking. If you strive to excel at lock icking, you will grow in many ways.

7.1 Mechanical Skills

Learning how to ull the ick over the ins is sur risingly difficult. The roblem is that the mechanical skills you learned early in life involved maintaining a fixed osition or fixed ath for your hands inde endent of the amount of force required. In lock icking, you must learn how to a ly a fixed force inde endent of the osition of your hand. As you ull the ick out of the lock you want to a ly a fixed ressure on the ins. The ick should bounce u and down in the keyway according to the resistance offered by each in.

To ick a lock you need feedback about the effects of your mani ulations. To get the feedback, you must train yourself to be sensitive to the sound and feel of the ick assing over the ins. This is a mechanical skill that can only be learned with ractice. The exercises will hel you recognize the im ortant information coming from your fingers.

7.2 Zen and the Art of Lock Picking

In order to excel at lock icking, you must train yourself to have a visually reconstructive imagination. The idea is to use information from all your senses to build a icture of what is ha ening inside the lock as you ick it. Basically, you want to roject your senses into the lock to receive a full icture of how it is res onding to your mani ulations. Once you have learned how to build this icture, it is easy to choose mani ulations that will o en the lock.

All your senses rovide information about the lock. Touch and sound rovide the most information, but the other senses can reveal critical information. For exam le, your nose can tell you whether a lock has been lubricated recently. As a beginner, you will need to use

your eyes for hand-eye coordination, but as you im rove you will find it unnecessary to look at the lock. In fact, it is better to ignore your eyes and use your sight to build an image of the lock based on the information you receive from your fingers and ears.

The goal of this mental skill is to acquire a relaxed concentration on the lock. Don't force the concentration. Try to ignore the sensations and thoughts that are not related to the lock. Don't try to focus on the lock.

7.3 Analytic Thinking

Each lock has its own s ecial characteristics which make icking harder or easier. If you learn to recognize and ex loit the " ersonality traits" of locks, icking will go much faster. Basically, you want to analyze the feedback you get from a lock to diagnose its ersonality traits and then use your ex erience to decide on an a roach to o en the lock. Cha ter 9 discusses a large number of common traits and ways to ex loit or overcome them.

Peo le underestimate the analytic skills involved in lock icking. They think that the icking tool o ens the lock. To them the torque wrench is a assive tool that just uts the lock under the desired stress. Let me ro ose another way to view the situation. The ick is just running over the ins to get information about the lock. Based on an analysis that information the torque is adjusted to make the ins set at the sheer line. It's the torque wrench that o ens the lock.

Varying the torque as the ick moves in and out of the keyway is a general trick that can be used to get around several icking roblems. For exam le, if the middle ins are set, but the end ins are not, you can increase the torque as the ick moves over the middle ins. This will reduce the chances of disturbing the correctly set ins. If some in doesn't seem to lift u far enough as the ick asses over it, then try reducing the torque on the next ass.

The skill of adjusting the torque while the ick is moving requires careful coordination between your hands, but as you become better at visualizing the rocess of icking a lock, you will become better at this im ortant skill.

Chapter 8

Exercises

This cha ter resents a series of exercises that will hel you learn the basic skill of lock icking. Some exercises teach a single skill, while others stress the coordination of skills.

When you do these exercises, focus on the skills, not on o ening the lock. If you focus on o ening the lock, you will get frustrated and your mind will sto learning. The goal of each exercise is to learn something about the articular lock you are holding and something about yourself. If a lock ha ens to o en, focus on the memory of what you were doing and what you felt just before it o ened.

These exercises should be racticed in short sessions. After about thirty minutes you will find that your fingers become sore and your mind looses its ability to achieve relaxed concentration.

8.1 Exercise 1: Bouncing the pick

This exercise hel s you learn the skill of a lying a fixed ressure with the ick inde endent of how the ick moves u and down in the lock. Basically you want to learn how to let the ick bounce u and down according to the resistance offered by each in.

How you hold the ick makes a difference on how easy it is to a ly a fixed ressure. You want to hold it in such a way that the ressure comes from your fingers or your wrist. Your elbow and shoulder do not have the dexterity required to ick locks. While you are scrubbing a lock notice which of your joints are fixed, and which are allowed to move. The moving joints are roviding the ressure.

One way to hold a ick is to use two fingers to rovide a ivot oint while another finger levers the ick to rovide the ressure. Which fingers you use is a matter of ersonal choice. Another way to hold the ick is like holding a encil. With this method, your wrist rovides the ressure. If your wrist is roviding the ressure, your shoulder and elbow should rovide the force to move the ick in and out of the lock. Do not use your wrist to both move the ick and a ly ressure.

A good way to get used to the feel of the ick bouncing u and down in the keyway is to try scrubbing over the ins of an o en lock. The ins cannot be ushed down, so the ick

must adjust to the heights of the ins. Try to feel the ins rattle as the ick moves over them. If you move the ick quickly, you can hear the rattle. This same rattling feel will hel you recognize when a in is set correctly. If a in a ears to be set but it doesn't rattle, then it is false set. False set ins can be fixed by ushing them down farther, or by releasing torque and letting them o back to their initial osition.

One last word of advice. Focus on the ti of the ick. Don't think about how you are moving the handle; think about how you are moving the ti of the ick.

8.2 Exercise 2: Picking pressure

This exercise will teach you the range of ressures you will need to a ly with a ick. When you are starting, just a ly ressure when you are drawing the ick out of the lock. Once you have mastered that, try a lying ressure when the ick is moving inward.

With the at side of your ick, ush down on the first in of a lock. Don't a ly any torque to the lock. The amount of ressure you are a lying should be just enough to overcome the s ring force. This force gives you an idea of minimum ressure you will a ly with a ick.

The s ring force increases as you ush the in down. See if you can feel this increase.

Now see how it feels to ush down the other ins as you ull the ick out of the lock. Start out with both the ick and torque wrench in the lock, but don't a ly any torque. As you draw the ick out of the lock, a ly enough ressure to ush each in all the way down.

The ins should s ring back as the ick goes ast them. Notice the sound that the ins make as they s ring back. Notice the o ing feel as a ick goes ast each in. Notice the s ringy feel as the ick ushes down on each new in.

To hel you focus on these sensations, try counting the number of ins in the lock. Door locks at MIT have seven ins, adlocks usually have four.

To get an idea of the maximum ressure, use the at side of your ick to ush down all the ins in the lock. Sometimes you will need to a ly this much ressure to a single in. If you encounter a new kind of lock, erform this exercise to determine the stiffness of its s rings.

8.3 Exercise 3: Picking Torque

This exercise will teach you the range of torque you will need to a ly to a lock. It demonstrates the interaction between torque and ressure which was describe in cha ter 5.

The minimum torque you will use is just enough to overcome the fiction of rotating the lug in the hull. Use your torque wrench to rotate the lug until it sto s. Notice how much torque is needed to move the lug before the ins bind. This force can be quite high for locks that have been left out in the rain. The minimum torque for adlocks includes the force of a s ring that is attached between the lug and the shackle bolt.

To get a feel for the maximum value of torque, use the at side of the ick to ush all the ins down, and try a lying enough torque to make the ins stay down after the ick is removed. If your torque wrench has a twist in it, you may not be able to hold down more than a few ins.

If you use too much torque and too much ressure you can get into a situation like the one you just created. The key ins are ushed too far into the hull and the torque is sufficient to hold them there.

The range of icking torque can be found by gradually increasing the torque while scrubbing the ins with the ick. Some of the ins will become harder to ush down. Gradually increase the torque until some of the ins set. These ins will loose their s ringiness. Kee ing the torque fixed, use the ick to scrub the ins a few times to see if other ins will set.

The most common mistake of beginners is to use too much torque. Use this exercise to find the minimum torque required to ick the lock.

8.4 Exercise 4: Identifying Set Pins

While you are icking a lock, try to identify which ins are set. You can tell a in is set because it will have a slight give. That is, the in can be ushed down a short distance with a light ressure, but it becomes hard to move after that distance (see cha ter 6 for an ex lanation). When you remove the light ressure, the in s rings back u slightly. Set ins also rattle if you ick them with the ick. Try listening for that sound.

Run the ick over the ins and try to decide whether the set ins are in the front or back of the lock (or both). Try identifying exactly which ins are set. Remember that in one is the frontmost in (i.e., the in that a key touches first). The most im ortant skill of lock icking is the ability to recognize correctly set ins. This exercise will teach you that skill.

Try re eating this exercise with the lug turning in the other direction. If the front ins set when the lug is turned one way, the back ins will set when the lug is turned the other way. See Figure 6.2 for an ex lanation.

One way to verify how many ins are set is to release the torque, and count the clicks as the ins sna back to their initial osition. Try this. Try to notice the difference in sound between the sna of a single in and the sna of two ins at once. A in that has been false set will also make a sna ing sound.

Try this exercise with different amounts of torque and ressure. You should notice that a larger torque requires a larger ressure to make ins set correctly. If the ressure is too high, the ins will be jammed into the hull and stay there.

8.5 Exercise 5: Projection

As you are doing the exercises try building a icture in your mind of what is going on. The icture does not have to be visual, it could be a rough understanding of which ins are set

and how much resistance you are encountering from each in. One way to foster this icture building is to try to remember your sensations and beliefs about a lock just before it o ened. When a lock o ens, don't think "that's over", think "what ha ened".

This exercise requires a lock that you find easy to ick. It will hel you refine the visual skills you need to master lock icking. Pick the lock, and try to remember how the rocess felt. Rehearse in your mind how everything feels when the lock is icked ro erly. Basically, you want to create a movie that records the rocess of icking the lock. Visualize the motion of your muscles as they a ly the correct ressure and torque, and feel the resistance encountered by the ick. Now ick the lock again trying to match your actions to the movie.

By re eating this exercise, you are learning how to formulate detailed commands for your muscles and how to inter ret feedback from your senses. The mental rehearsal teaches you how to build a visual understanding of the lock and how to recognize the major ste s of icking it.

Chapter 9

Recog ízi g a Exp oíti g Perso a ity Traits

Real locks have a wide range of mechanical features and defects that hel and hinder lock icking. If a lock doesn't res ond to scrubbing, then it robably has one of the traits discussed in this cha ter. To o en the lock, you must diagnose the trait and a ly the recommended technique. The exercises will hel you develo the mechanical sensitivity and dexterity necessary to recognize and ex loit the different traits.

9.1 Which Way To Turn

It can be very frustrating to s end a long time icking a lock and then discover that you turned the lug the wrong way. If you turn a lug the wrong way it will rotate freely until it hits a sto , or until it rotates 180 degrees and the drivers enter the keyway (see section 9.11). Section 9.11 also ex lains how to turn the lug more than 180 degrees if that is necessary to fully retract the bolt. When the lug is turned in the correct direction, you should feel an extra resistance when the lug cam engages the bolt s ring.

The direction to turn the lug de ends on the bolt mechanism, not on the lock, but here are some general rules. Chea adlocks will o en if the lug is turned in either direction, so you can chose the direction which is best for the torque wrench. All adlocks made by the Master com any can be o ened in either direction. Padlocks made by Yale will only o en if the lug is turned clockwise. The double lug Yale cylinder locks generally o en by turning the bottom of the keyway (i.e., the at edge of the key) away from the nearest doorframe. Single lug cylinder locks also follow this rule. See Figure 9.1. Locks built into the doorknob usually o en clockwise. Desk and filing cabinet locks also tend to o en clockwise.

When you encounter a new kind of lock mechanism, try turning the lug in both directions. In the correct direction, the lug will be sto ed by the ins, so the sto will feel mushy when you use heavy torque. In the wrong direction the lug will be sto ed by a metal tab, so the sto will feel solid.

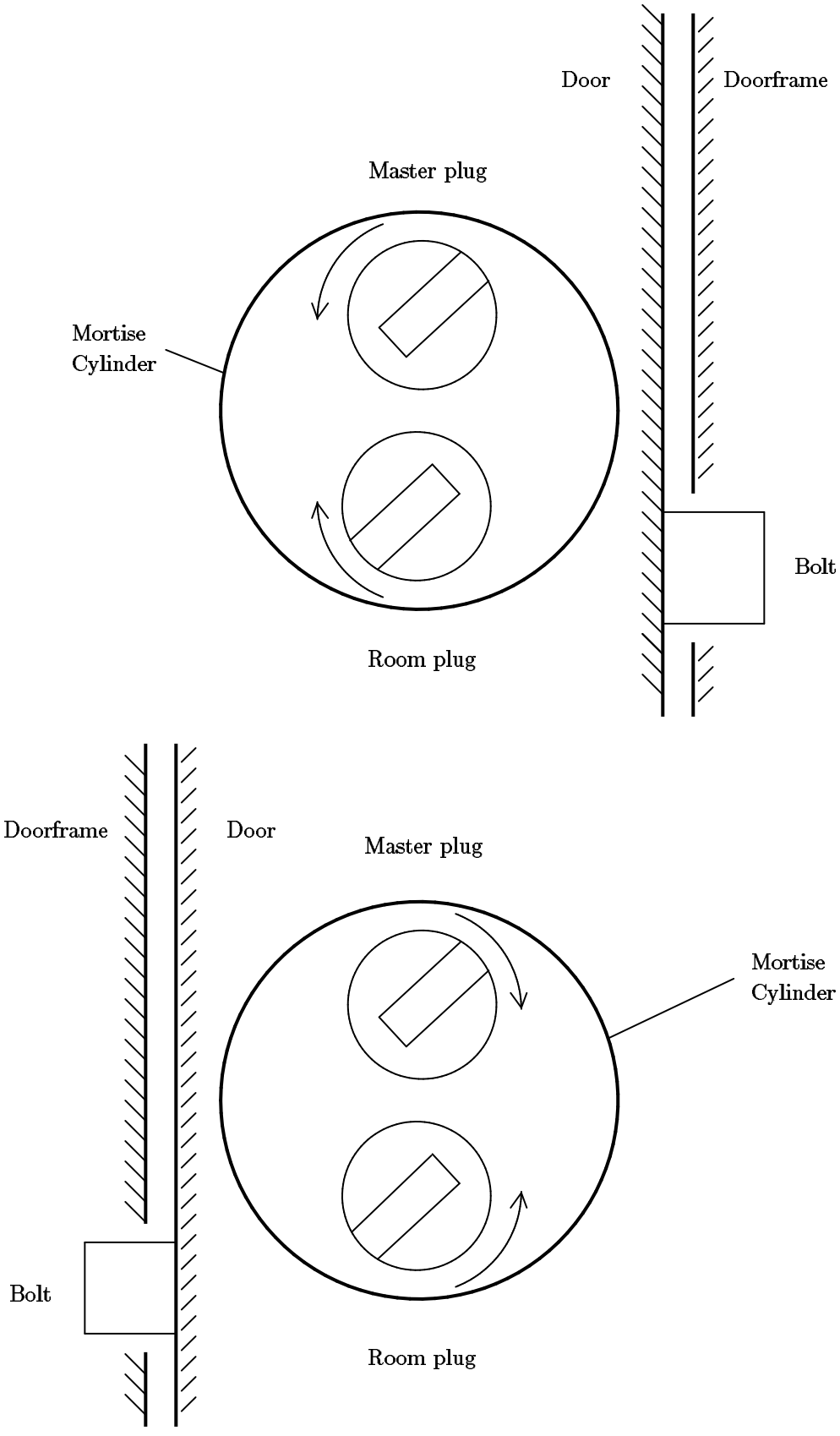


Figure 9.1: Direction to turn lug

9.2 How Far to Turn

The com anion question to which way to turn a lock is how far to turn it. Desk and filing cabinet locks generally o en with less than a quarter turn (90 degrees) of the lug. When o ening a desk lock try to avoid having the lug lock in the o en osition. Locks built into doorknobs also tend to o en with less than a quarter turn. Locks which are se arate from the doorknob tend to require a half turn to o en. Deadbolt lock mechanisms can require almost a full turn to o en.

Turning a lock more than 180 degrees is a difficult because the drivers enter the bottom of the keyway. See section 9.11.

9.3 Gravity

Picking a lock that has the s rings at the to is different than icking one with the s rings at the bottom. It should be obvious how to tell the two a art. The nice feature of a lock with the s rings at the bottom is that gravity holds the key ins down once they set. With the set ins out of the way, it is easy to find and mani ulate the remaining unset ins. It is also straight forward to test for the slight give of a correctly set in. When the s rings are on to , gravity will ull the key ins down after the driver in catches at the sheer line. In this case, you can identify the set ins by noticing that the key in is easy to lift and that it does not feel s ringy. Set ins also rattle as you draw the ick over them because they are not being ushed down by the driver in.

9.4 Pins Not Setting

If you scrub a lock and ins are not setting even when you vary the torque, then some in has false set and it is kee ing the rest of the ins from setting. Consider a lock whose ins refer to set from back to front. If the backmost in false sets high or low (see Figure 9.2), then the lug cannot rotate enough to allow the other ins to bind. It is hard to recognize that a back in has false set because the s ringiness of the front ins makes it hard to sense the small give of a correctly set back in. The main sym tom of this situation is that the other ins will not set unless a very large torque is a lied.

When you encounter this situation, release the torque and start over by concentrating on the back ins. Try a light torque and moderate ressure, or heavy torque and heavy ressure. Try to feel for the click that ha ens when a in reaches the sheer line and the lug rotates slightly. The click will be easier to feel if you use a stiff torque wrench.

9.5 Elastic Deformation

The interesting events of lock icking ha en over distances measured in thousandths of an inch. Over such short distances, metals behave like s rings. Very little force is necessary

to de ect a iece metal over those distances, and when the force is removed, the metal will s ring back to its original osition.

Deformation can be used to your advantage if you want to force several ins to bind at once. For exam le, icking a lock with ins that refer to set from front to back is slow because the ins set one at a time. This is articularly true if you only a ly ressure as the ick is drawn out of the lock. Each ass of the ick will only set the frontmost in that is binding. Numerous asses are required to set all the ins. If the reference for setting is not very strong (i.e., the axis of the lug holes is only slightly skewed from the lug's center line), then you can cause additional ins to bind by a lying extra torque. Basically, the torque uts a twist in the lug that causes the front of the lug to be de ected further than the back of the lug. With light torque, the back of the lug stays in its initial osition, but with medium to heavy torque, the front in columns bend enough to allow the back of the lug to rotate and thus cause the back ins to bind. With the extra torque, a single stroke of the ick can set several ins, and the lock can be o ened quickly. Too much torque causes its own roblems.

When the torque is large, the front ins and lug holes can be deformed enough to revent the ins from setting correctly. In articular, the first in tends to false set low. Figure 9.2 shows how excess torque can deform the bottom of the driver in and revent the key in from reaching the sheer line. This situation can be recognized by the lack of give in the first in. Correctly set ins feel s ringy if they are ressed down slightly. A falsely set in lacks this s ringiness. The solution is to ress down hard on the first in. You may want to reduce the torque slightly, but if you reduce torque too much then other ins will unset as the first in is being de ressed.

It is also ossible to deform the to of the key in. The key in is scissored between the lug and the hull and stays fixed. When this ha ens, the in is said to be false set high.

9.6 Loose Plug

The lug is held into the hull by being wider at the front and by having a cam on the back that is bigger than the hole drilled into the hull. If the cam is not ro erly installed, the lug can move in and out of the lock slightly. On the outward stroke of the ick, the lug will move forward, and if you a ly ressure on the inward stroke, the lug will be ushed back.

The roblem with a loose lug is that the driver ins tend to set on the back of the lug holes rather than on the sides of the holes. When you ush the lug in, the drivers will unset. You can use this defect to your advantage by only a lying ressure on the outward or inward stroke of the ick. Alternatively, you can use your finger or torque wrench to revent the lug from moving forward.

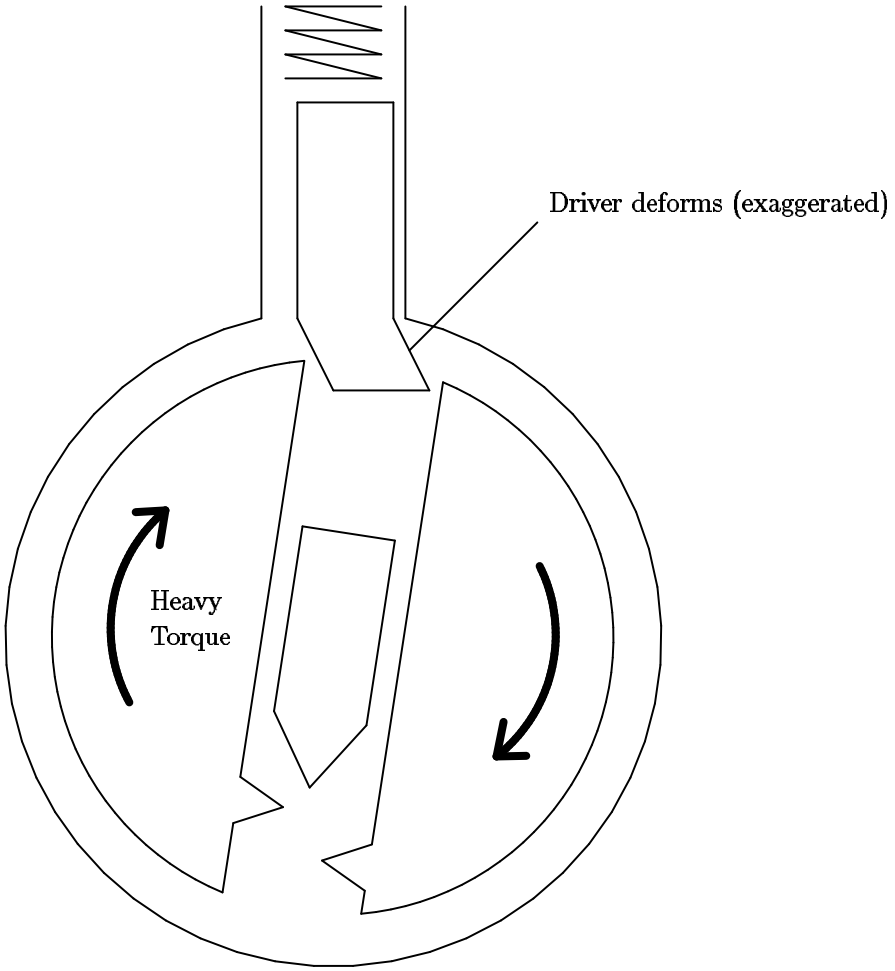


Figure 9.2: Driver in false set by elastic deformation

9.7 Pin Diameter

When the air of ins in a articular column have different diameters, that column will react strangely to the ressure of the ick.

The to half of Figure 9.3 shows a in column with a driver in that has a larger diameter than the key in. As the ins are lifted, the icking ressure is resisted by the binding friction and the s ring force. Once the driver clears the sheer line, the lug rotates (until some other in binds) and the only resistance to motion is the s ring force. If the key in is small enough and the lug did not rotate very far, the key in can enter the hull without colliding with the edge of the hull. Some other in is binding, so again the only resistance to motion is the s ring force. This relationshi is gra hed in the bottom half of the Figure. Basically, the ins feel normal at first, but then the lock clicks and the in becomes s ringy. The narrow key in can be ushed all the way into the hull without loosing its s ringiness, but when the icking ressure is released, the key in will fall back to its initial osition while the large driver catches on the edge of the lug hole.

The roblem with a large driver in is that the key in tends to get stuck in the hull when some other in sets. Imagine that a neighboring in sets and the lug rotates enough to bind the narrow key in. If the ick was ressing down on the narrow key in at the same time as it was ressing down on the in that set, then the narrow key in will be in the hull and it will get stuck there when the lug rotates.

The behavior of a large key in is left as an exercise for the reader.

9.8 Beveled Holes and Rounded pins

Some lock manufacturers (e.g., Yale) bevel the edges of the lug holes and/or round off the ends of the key ins. This tends to reduce the wear on the lock and it can both hel and hinder lock icking. You can recognize a lock with these features by the large give in set ins. See Figure 9.4. That is, the distance between the height at which the driver in catches on the edge of the lug hole and the height at which the key in hits the hull is larger (sometimes as large as a sixteenth of an inch) when the lug holes are beveled or the ins are rounded. While the key in is moving between those two heights, the only resistance to motion will be the force of the s ring. There won't be any binding friction. This corres onds to the di in the force gra h shown in Figure 5.5.

A lock with beveled lug holes requires more scrubbing to o en than a lock without beveled holes because the driver ins set on the bevel instead of setting on the to of the lug. The lug will not turn if one of the drivers is caught on a bevel. The key in must be scrubbed again to ush the driver in u and off the bevel. The left driver in in Figure 9.6a is set. The driver is resting on the bevel, and the bottom late has moved enough to allow the right driver to bind. Figure 9.6b shows what ha ens after the right driver in sets. The bottom late slides further to the right and now the left driver in is scissored between the bevel and the to late. It is caught on the bevel. To o en the lock, the left driver in must be ushed u above the bevel. Once that driver is free, the bottom late

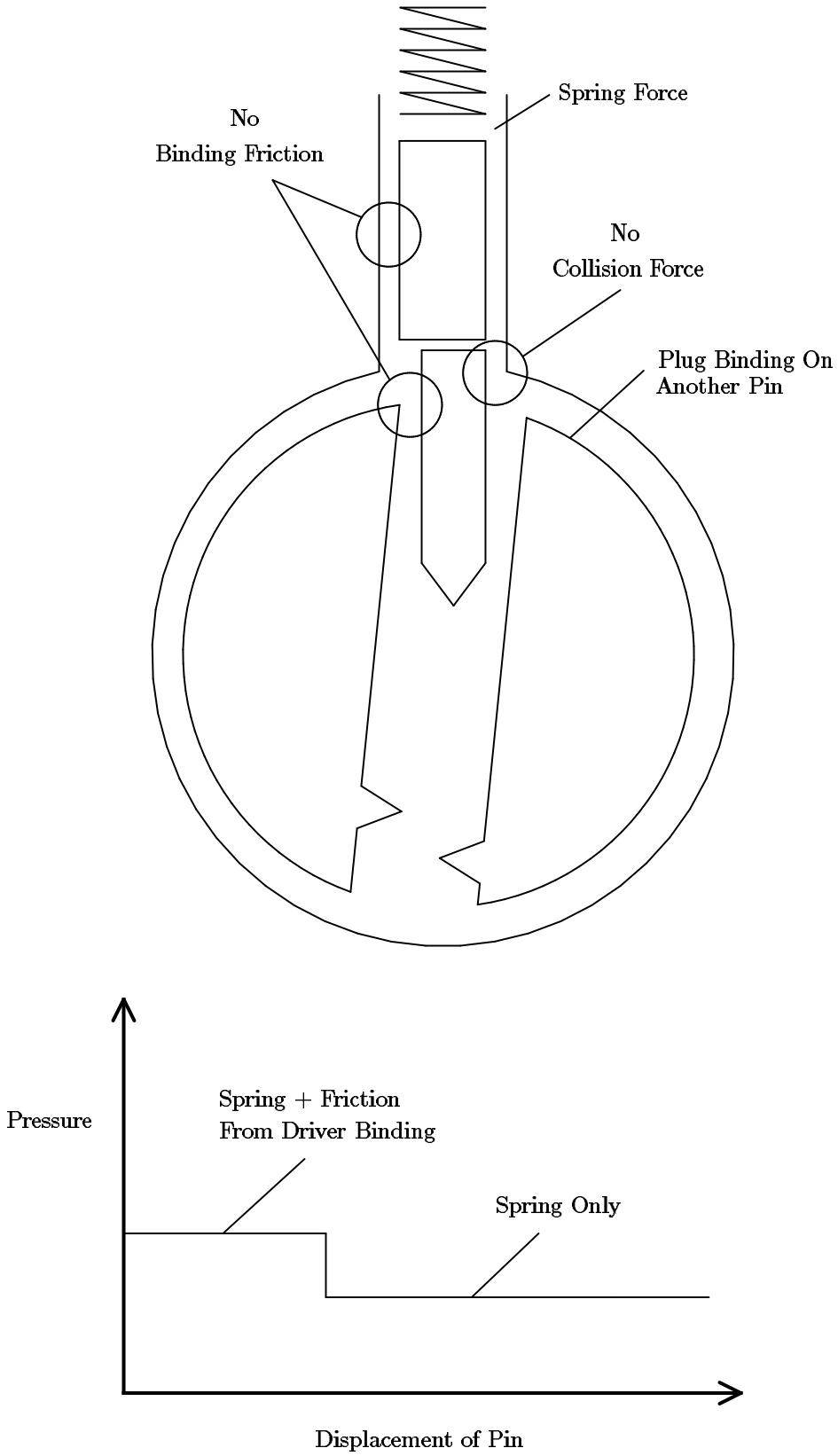


Figure 9.3: Driver in wider than key in

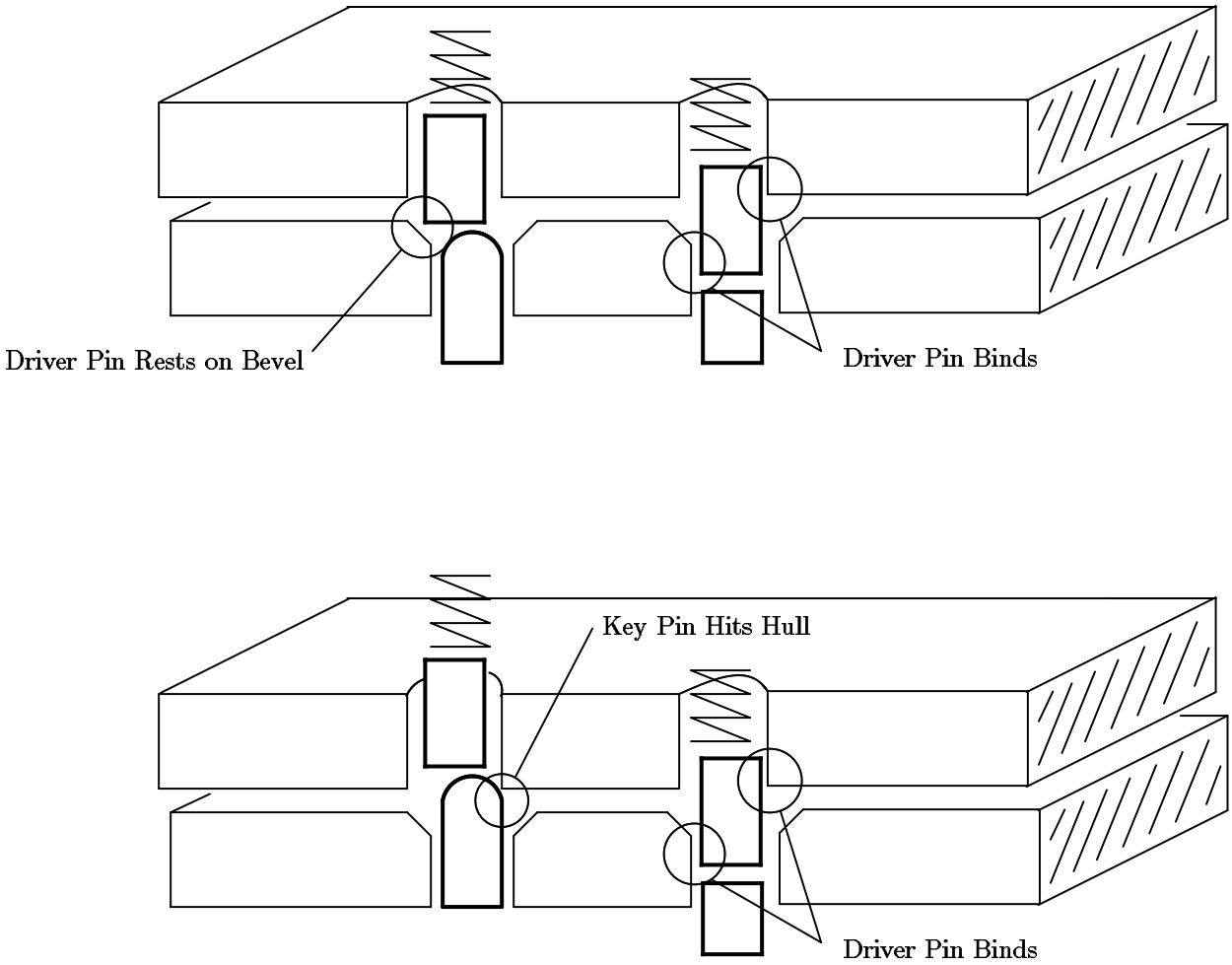


Figure 9.4: Beveled lug holes and rounded key ins

can slide and the right driver may bind on its bevel.

If you encounter a lock with beveled lug holes, and all the ins a ear to be set but the lock is not o ening, you should reduce torque and continue scrubbing over the ins. The reduced torque will make it easier to ush the drivers off the bevels. If ins unset when you reduce the torque, try increasing the torque and the icking ressure. The roblem with increasing the force is that you may jam some key ins into the hull.

9.9 Mushroom Driver Pins

A general trick that lock makers use to make icking harder is to modify the sha e of the driver in. The most o ular sha es are mushroom, s ool and serrated, see Figure 9.7. The ur ose of these sha es is to cause the ins to false set low. These drivers sto a icking technique called vibration icking (see section 9.12), but they only slightly com licate scrubbing and one- in-at-a-time icking (see cha ter 4).

If you ick a lock and the lug sto s turning after a few degrees and none of the ins

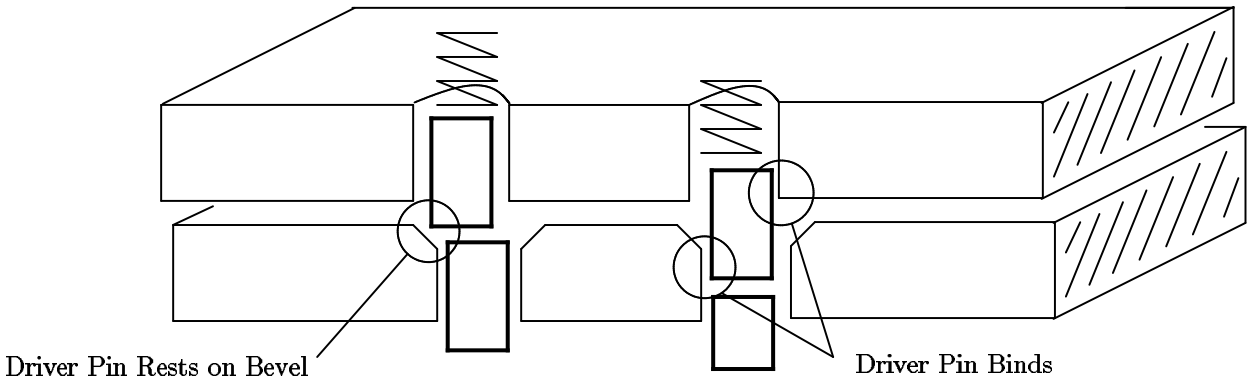


Figure 9.5: (a) Driver sets on bevel

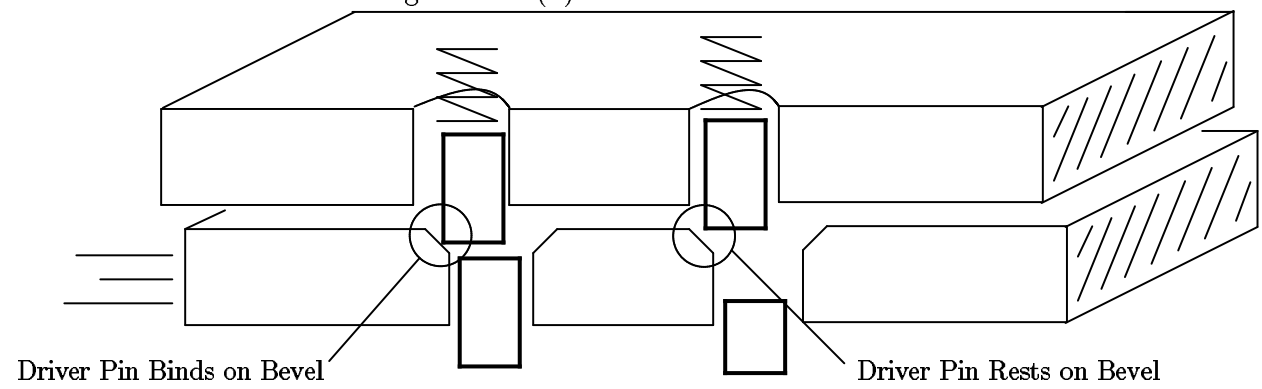


Figure 9.6: (b) Driver jams on bevel

can be ushed u any further, then you known that the lock has modified drivers. Basically, the li of the driver has caught at the sheer line. See the bottom of Figure 9.7. Mushroom and s ool drivers are often found in Russwin locks, and locks that have several s acers for master keying.

You can identify the ositions with mushroom drivers by a lying a light torque and ushing u on each in. The ins with mushroom drivers will exhibit a tendency to bring the lug back to the fully locked osition. By ushing the key in u you are ushing the at to of the key in against the tilted bottom of the mushroom driver. This causes the driver to straighten u which in turn causes the lug to unrotate. You can use this motion to identify the columns that have mushroom drivers. Push those ins u to sheer line; even if you lose some of the other ins in the rocess they will be easier to re- ick than the ins with mushroom drivers. Eventually all the ins will be correctly set at the sheer line.

One way to identify all the ositions with mushroom drivers is to use the at of your ick to ush all the ins u about halfway. This should ut most of the drivers in their cockable osition and you can feel for them.

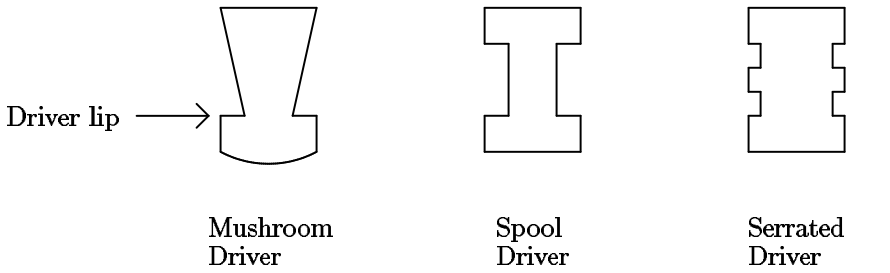
To ick a lock with modified drivers, use a lighter torque and heavier ressure. You want to error on the side of ushing the key ins too far into the hull. In fact, another way to ick these locks is to use the at side of your ick to ush the ins u all the way, and a ly very heavy torque to hold them there. Use a scrubbing action to vibrate the key ins while you slowly reduce the torque. Reducing the torque reduces the binding friction on the ins. The vibration and s ring force cause the key ins to slide down to the sheer line.

The key to icking locks with modified drivers is recognizing incorrectly set ins. A mushroom driver set on its li will not have the s ringy give of a correctly set driver. Practice recognizing the difference.

9.10 Master Keys

Many a lications require keys that o en only a single lock and keys that o en a grou of locks. The keys that o en a single lock are called *change keys* and the keys that o en multi le locks are called *master keys*. To allow both the change key and the master key to o en the same lock, a locksmith adds an extra in called a *spacer* to some of the in columns. See Figure 9.8. The effect of the s acer is to create two ga s in the in column that could be lined u with the sheer line. Usually the change key aligns the to of the s acer with the sheer line, and the master key aligns the bottom of the s acer with the sheer line (the idea is to revent eo le from filing down a change key to get a master key). In either case the lug is free to rotate.

In general, s acers make a lock easier to ick. They increase the number of o ortunities to set each in, and they make it more likely that the lock can o ened by setting the all the ins at about the same height. In most cases only two or three ositions will have s acers. You can recognize a osition with a s acer by the two clicks you feel when the in is ushed down. If the s acer has a smaller diameter than the driver and key ins, then you will feel a wide s ringy region because the s acer will not bind as it asses through the sheer line. It is



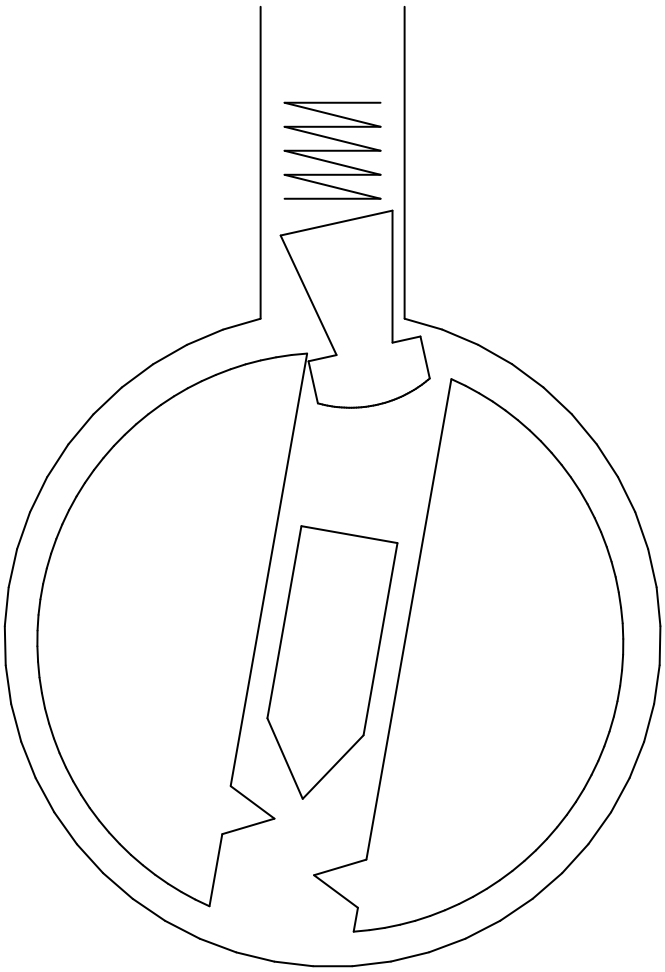


Figure 9.7: Mushroom, s ool, and serrated driver ins

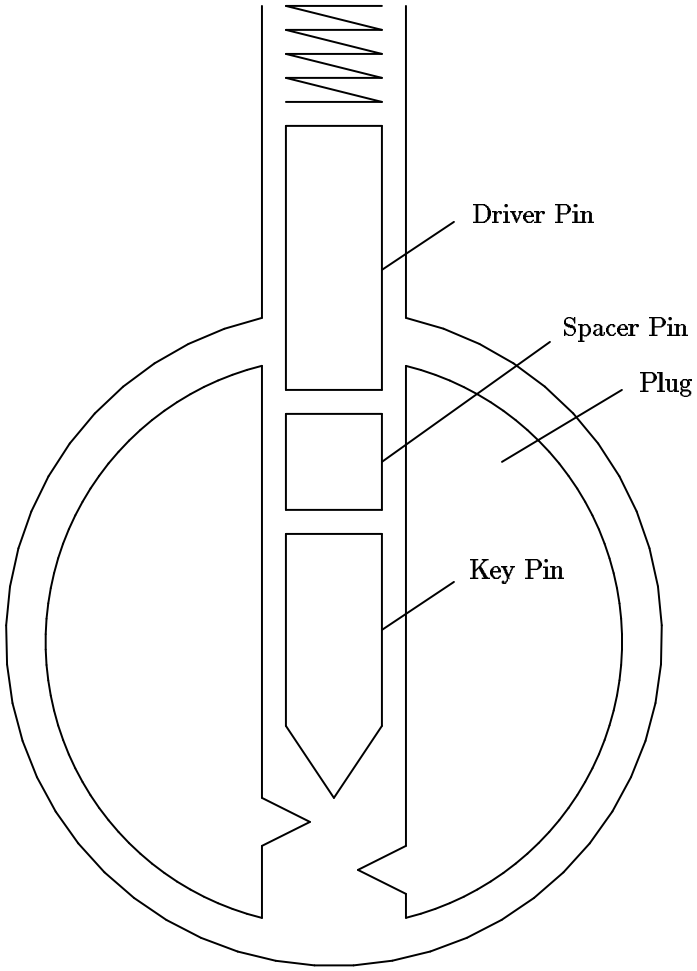


Figure 9.8: S acer ins for master keying

more common for the s acer to be larger than the driver in. You can recognize this by an increase in friction when the s acer asses through the sheer line. Since the s acer is larger than the driver in, it will also catch better on the lug. If you ush the s acer further into the hull, you will feel a strong click when the bottom of the s acer clears the sheer line.

Thin s acers can cause serious roblems. If you a ly heavy torque and the lug has beveled holes, the s acer can twist and jam at the sheer line. It is also ossible for the s acer to fall into the keyway if the lug is rotated 180 degrees. See section 9.11 for the solution to this roblem.

9.11 Driver or Spacer Enters Keyway

Figure 9.9 shows how a s acer or driver in can enter the keyway when the lug is rotated 180 degrees. You can revent this by lacing the at side of your ick in the bottom of the keyway **before** you turn the lug too far. If a s acer or driver does enter the keyway and revent you from turning the lug, use the at side of you ick to ush the s acer back into

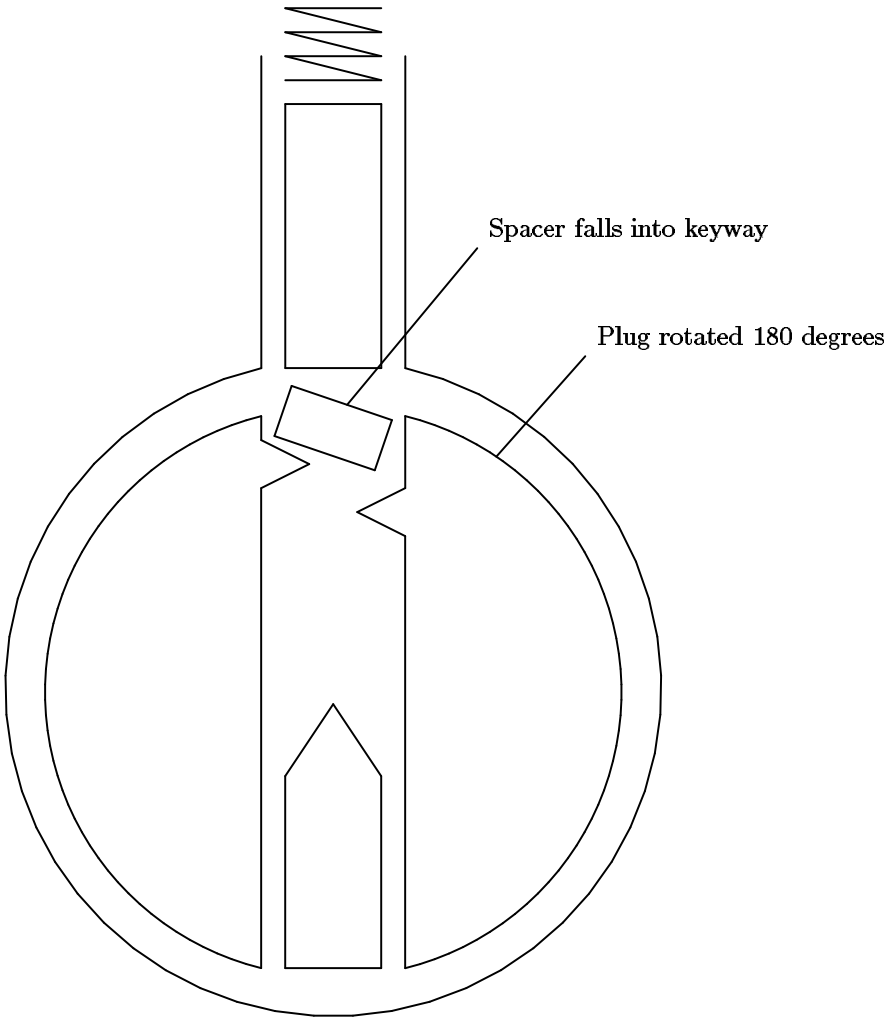


Figure 9.9: S acer or driver can enter keyway

the hull. You may need to use the torque wrench to relieve any sheer force that is binding the s acer or driver. If that doesn't work try raking over the drivers with the ointed side of your ick. If a s acer falls into the keyway com letely, the only o tion is to remove it. A hook sha ed iece of s ring steel works well for this, though a bent a ercli will work just as well unless the s acer becomes wedged.

9.12 Vibration Picking

Vibration icking works by creating a large ga between the key and driver ins. The underlying rinci le is familiar to anyone who has layed ool. When the queue ball strikes another ball squarely, the queue ball sto s and the other ball heads off with the same s eed and direction as the queue ball. Now imagine a device that kicks the ti s of all the key ins. The key ins would transfer their momentum to the driver ins which would y u into the hull. If you are a lying a light torque when this ha ens, the lug will rotate when all the

drivers are above the sheer line.

9.13 Disk Tumblers

The inex ensive locks found on desks use metal disks instead of ins. Figure 9.10 shows the basic workings of these locks. The disks have the same outline but differ in the lacement of the rectangular cut.

These locks are easy to ick with the right tools. Because the disks are laced close together a half-round ick works better than a half-diamond ick (see Figure A.1). You may also need a torque wrench with a narrower head. Use moderate to heavy torque.

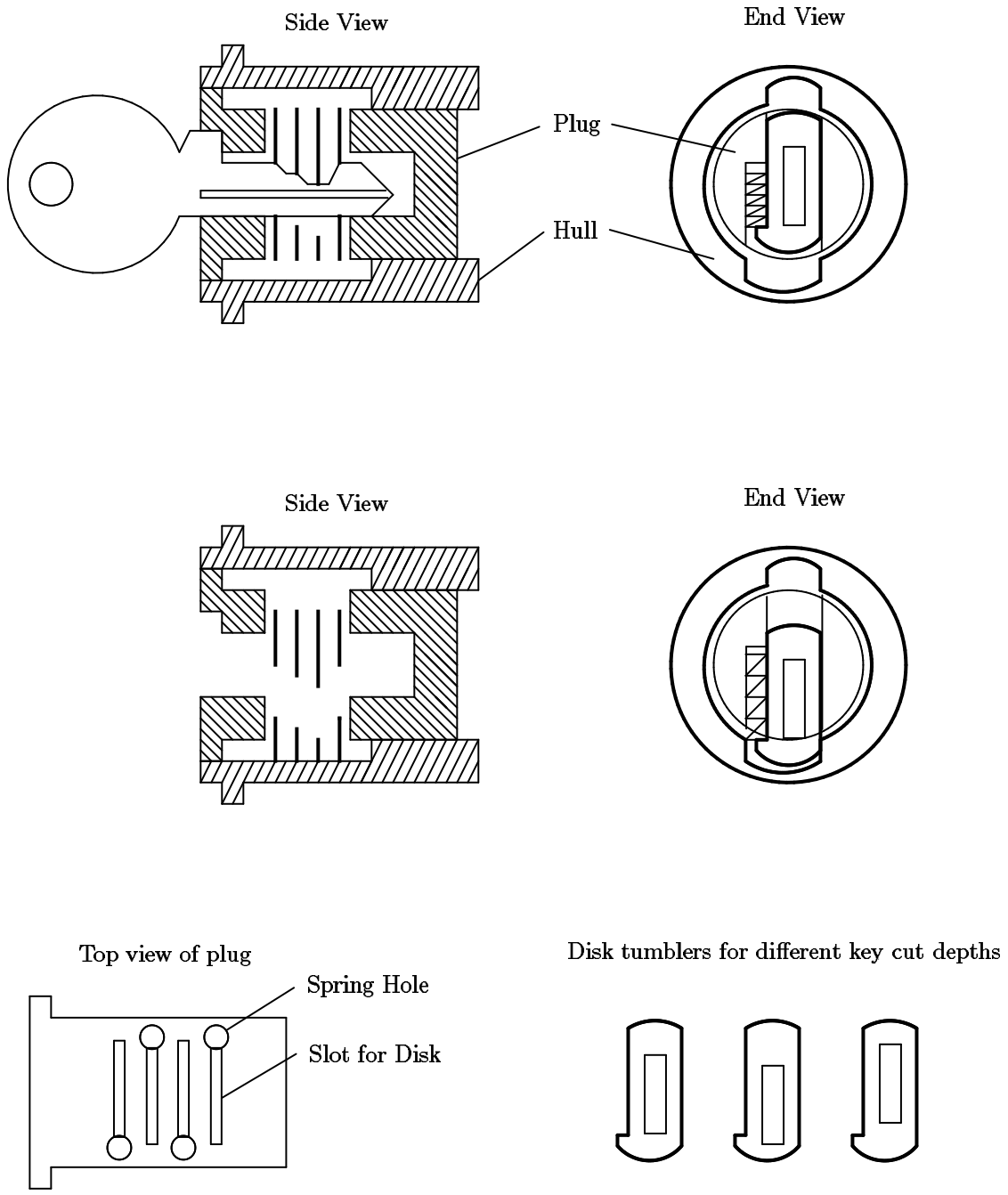


Figure 9.10: Workings of a disk tumbler lock

Chapter 10

Fi a Remarks

Lock icking is a craft, not a science. This document resents the knowledge and skills that are essential to lock icking, but more im ortantly it rovides you with models and exercises that will hel you study locks on your own. To excel at lock icking, you must ractice and develo a style which fits you ersonally. Remember that the best technique is the one that works best for you.

Appe ix A

Too s

This a endix describes the design and construction of lock icking tools.

A.1 Pick Shapes

Picks come in several sha es and sizes. Figure A.1 shows the most common sha es. The handle and tang of a ick are the same for all icks. The handle must be comfortable and the tang must be thin enough to avoid bum ing ins unnecessarily. If the tang is too thin, then it will act like a s ring and you will loose the feel of the ti interacting with the ins. The sha e of the ti determines how easily the ick asses over the ins and what kind of feedback you get from each in.

The design of a ti is a com romise between ease of insertion, ease of withdrawal and feel of the interaction. The half diamond ti with shallow angles is easy to insert and remove, so you can a ly ressure when the ick is moving in either direction. It can quickly ick a lock that has little variation in the lengths of the key ins. If the lock requires a key that has a dee cut between two shallow cuts, the ick may not be able to ush the middle in down far enough. The half diamond ick with stee angles could deal with such a lock, and in general stee angles give you better feedback about the ins. Unfortunately, the stee angles make it harder to move the ick in the lock. A ti that has a shallow front angle and a stee back angle works well for Yale locks.

The half round ti works well in disk tumbler locks. See section 9.13. The full diamond and full round ti s are useful for locks that have ins at the to and bottom of the keyway.

The rake ti is designed for icking ins one by one. It can also be used to rake over the ins, but the ressure can only be a lied as the ick is withdrawn. The rake ti allows you to carefully feel each in and a ly varying amounts of ressure. Some rake ti s are at or dented on the to to makes it easier to align the ick on the in. The rimary benefit of icking ins one at a time is that you avoid scratching the ins. Scrubbing scratches the ti s of the ins and the keyway, and it s reads metal dust throughout the lock. If you want to avoid leaving traces, you must avoid scrubbing.

The snake ti can be used for scrubbing or icking. When scrubbing, the multi le bum s

generate more action than a regular ick. The snake ti is articularly good at o ening five in household locks. When a snake ti is used for icking, it can set two or three ins at once. Basically, the snake ick acts like a segment of a key which can be adjusted by lifting and lowering the ti , by tilting it back and forth, and by using either to to or bottom of the ti . You should use moderate to heavy torque with a snake ick to allow several ins to bind at the same time. This style of icking is faster than using a rake and it leaves as little evidence.

A.2 Street cleaner bristles

The s ring steel bristles used on street cleaners make excellent tools for lock icking. The bristles have the right thickness and width, and they are easy to grind into the desired sha e. The resulting tools are s ringy and strong. Section A.3 describes how to make tools that are less s ringy.

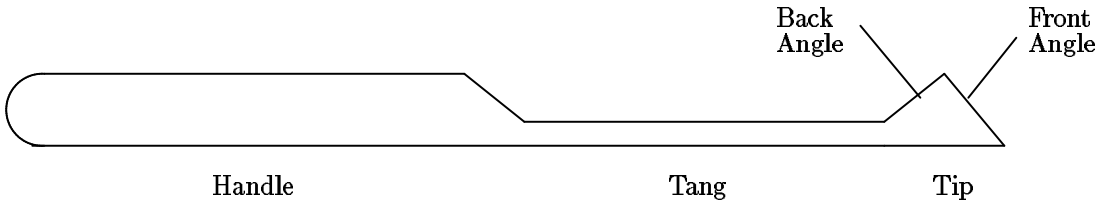
The first ste in making tools is to sand off any rust on the bristles. Course grit sand a er works fine as does a steel wool cleaning ad (not co er wool). If the edges or ti of the bristle are worn down, use a file to make them square.

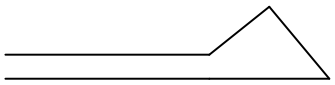
A torque wrench has a head and a handle as shown in figure A.2. The head is usually 1/2 to 3/4 of an inch long and the handle varies from 2 to 4 inches long. The head and the handle are se arated by a bend that is about 80 degrees. The head must be long enough to reach over any rotrusions (such as a gri - roof collar) and firmly engage the lug. A long handle allows delicate control over the torque, but if it is too long, it will bum against the doorframe. The handle, head and bend angle can be made quite small if you want to make tools that are easy to conceal (e.g., in a en, ashlight, or belt buckle). Some torque wrenches have a 90 degree twist in the handle. The twist makes it easy to control the torque by controlling how far the handle has been de ected from its rest osition. The handle acts as a s ring which sets the torque. The disadvantage of this method of setting the torque is that you get less feedback about the rotation of the lug. To ick difficult locks you will need to learn how to a ly a steady torque via a stiff handled torque wrench.

The width of the head of a torque wrench determines how well it will fit the keyway. Locks with narrow keyways (e.g., desk locks) need torque wrenches with narrow heads. Before bending the bristle, file the head to the desired width. A general ur ose wrench can be made by narrowing the ti (about 1/4 inch) of the head. The ti fits small keyways while the rest of the head is wide enough to grab a normal keyway.

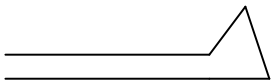
The hard art of making a torque wrench is bending the bristle without cracking it. To make the 90 degree handle twist, clam the head of the bristle (about one inch) in a vise and use liers to gras the bristle about 3/8 of an inch above the vise. You can use another air of liers instead of a vise. A ly a 45 degree twist. Try to kee the axis of the twist lined u with the axis of the bristle. Now move the liers back another 3/8 inch and a ly the remaining 45 degrees. You will need to twist the bristle more than 90 degrees in order to set a ermanent 90 degree twist.

To make the 80 degree head bend, lift the bristle out of the vise by about 1/4 inch (so

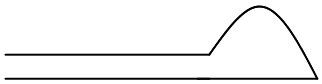




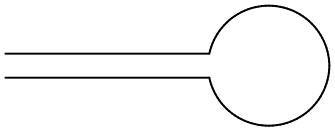
Half Diamond
Shallow Angles



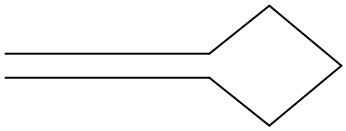
Half Diamond
Steep Angles



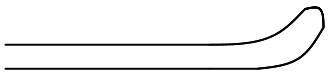
Half Round



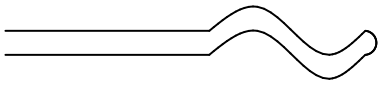
Full Round



Full Diamond



Rake



Snake

Figure A.1: Selection of ick sha es

3/4 inch is still in the vise). Place the shank of a screw driver against the bristle and bend the s ring steel around it about 90 degrees. This should set a ermanent 80 degree bend in the metal. Try to kee the axis of the bend er endicular to the handle. The screwdriver shank ensures that the radius of curvature will not be too small. Any rounded object will work (e.g., drill bit, needle nose liers, or a en ca). If you have trouble with this method, try gras ing the bristle with two liers se arated by about 1/2 inch and bend. This method roduces a gentle curve that won't break the bristle.

A grinding wheel will greatly s eed the job of making a ick. It takes a bit of ractice to learn how make smooth cuts with a grinding wheel, but it takes less time to ractice and make two or three icks than it does to hand file a single ick. The first ste is to cut the front angle of the ick. Use the front of the wheel to do this. Hold the bristle at 45 degrees to the wheel and move the bristle side to side as you grind away the metal. Grind slowly to avoid overheating the metal, which makes it brittle. If the metal changes color (to dark blue), you have overheated it, and you should grind away the colored ortion. Next, cut the back angle of the ti using the corner of the wheel. Usually one corner is shar er than the other, and you should use that one. Hold the ick at the desired angle and slowly ush it into the corner of the wheel. The side of the stone should cut the back angle. Be sure that the ti of the ick is su orted. If the grinding wheel stage is not close enough to the wheel to su ort the ti , use needle nose liers to hold the ti . The cut should should ass though about 2/3 of the width of the bristle. If the ti came out well, continue. Otherwise break it off and try again. You can break the bristle by clam ing it into a vise and bending it shar ly.

The corner of the wheel is also used to grind the tang of the ick. Put a scratch mark to indicate how far back the tang should go. The tang should be long enough to allow the ti to ass over the back in of a seven in lock. Cut the tang by making several smooth asses over the corner. Each ass starts at the ti and moves to the scratch mark. Try to remove less than a 1/16th of an inch of metal with each ass. I use two fingers to hold the bristle on the stage at the ro er angle while my other hand ushes the handle of the ick to move the tang along the corner. Use whatever technique works best for you.

Use a hand file to finish the ick. It should feel smooth if you run a finger nail over it. Any roughness will add noise to the feedback you want to get from the lock.

The outer sheath of hone cable can be used as a handle for the ick. Remove three or four of the wires from a length of cable and ush it over the ick. If the sheath won't stay in lace, you can ut some e oxy on the handle before ushing the sheath over it.

A.3 Bicycle sp◌okes

An alternative to making tools out of street cleaner bristles is to make them out of nails and bicycle s okes. These materials are easily accessible and when they are heat treated, they will be stronger than tools made from bristles.

A strong torque wrench can be constructed from an 8- enny nail (about .1 inch diameter). First heat u the oint with a ro ane torch until it glows red, slowly remove it from the

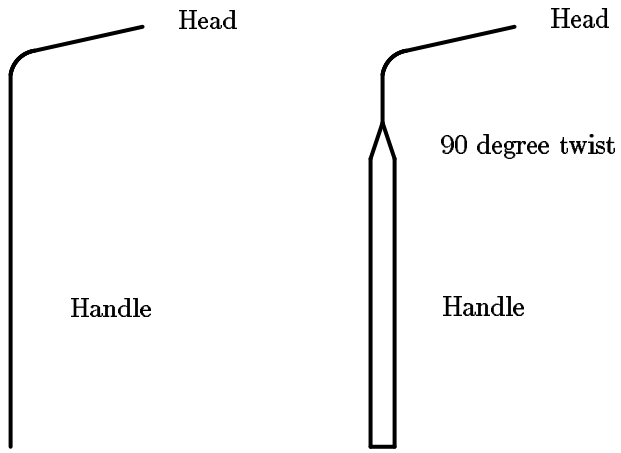


Figure A.2: Torque wrenches

ame, and let it air cool; this softens it. The burner of a gas stove can be used instead of a torch. Grind it down into the sha e of a skinny screwdriver blade and bend it to about 80 degrees. The bend should be less than a right angle because some lock faces are recessed behind a late (called an *escutcheon*) and you want the head of the wrench to be able to reach about half an inch into the lug. Tem er (harden) the torque wrench by heating to bright orange and dunking it into ice water. You will wind u with a virtually indestructible bent screwdriver that will last for years under brutal use.

Bicycle s okes make excellent icks. Bend one to the sha e you want and file the sides of the business end at such that it's strong in the vertical and exy in the horizontal direction. Try a right-angle hunk about an inch long for a handle. For smaller icks, which you need for those really tiny keyways, find any large-diameter s ring and unbend it. If you're careful you don't have to lay any metallurgical games.

A.4 Brick Strap

For erfectly serviceable key blanks that you can't otherwise find at the store, use the metal stra they wra around bricks for shi ing. It's wonderfully handy stuff for just about anything you want to manufacture. To get around side wards in the keyway, you can bend the stra lengthwise by clam ing it in a vice and ta ing on the rotruding art to bend the iece to the required angle.

Brick stra is very hard. It can ruin a grinding wheel or key cutting machine. A hand file is the recommended tool for milling brick stra .

Appe ix B

Lega Issues

Contrary to wides read myth, it is not a felony to ossess lock icks. Each state has its own laws with res ect to such burglarious instruments. Here is the Massachusetts version quoted in entirety from the massachusetts general code:

Cha ter 266 (crimes against ro erty)
Section 49. Burglarious instruments; making; ossession; use.

> Whoever makes or mends, or begins to make or mend, or knowingly has in his ossession, an engine, machine, tool or im lement ada ted and designed for cutting through, forcing or breaking o en a building, room, vault, safe or other de ository, IN ORDER TO STEAL THEREFROM money or other ro erty, or to commit any other crime, knowing the same to be ada ted and designed for the ur ose aforesaid, WITH INTENT TO USE OR EMPLOY OR ALLOW the same to be used or em loyed for such ur ose, or whoever knowingly has in his ossession a master key designed to fit more than one motor vehicle, WITH INTENT, TO USE OR EMPLOY THE SAME to steal a motor vehicle or other ro erty therefrom, shall be unished by im risonment in the state rison for not more than ten years or by a fine of not more than one thousand dollars and im risonment in jail for not more than two and one half years.

Em hasis added.

In other words, mere ossession means nothing. If they sto you for s eeding or something, and find a ick set, they can't do much. On the other hand, if they catch you icking the lock on a Monec machine they get to draw and quarter you.

States with similar wording include ME, NH, NY. One lace that DOES NOT have similar wording, and does make ossession illegal, is Washington, DC. These are the only other laces I have checked. I would imagine that most states are similar to Massachusetts, but I would not bet anything substantial (say, more than a slice of izza) on it.

It may be a good idea to carry around a xeroxed co y of the a ro riate age from your state's criminal code.